Відомості про автора

КОЛЕСНИК Тетяна Василівна – кандидат економічних наук, доцент кафедри адміністративного менеджменту та альтернативних джерел енергії, Вінницький національний аграрний університет (21008, м. Вінниця, вул. Сонячна 3, e-mail: sergej.kolesnik@gmail.com).

KOLESNIK Tatyana – Candidate of Economic Sciences, Associate Professor of the Department of Administrative Management and Alternative Energy Sources, Vinnytsia National Agrarian University (21008, Vinnytsia, 3 Soniachna St., e-mail: sergej.kolesnik@gmail.com).

КОЛЕСНИК Татьяна Васильевна – кандидат экономических наук, доцент кафедры административного менеджмента и альтернативных источников энергии, Винницкий национальный аграрный университет (21008, г. Винница, ул. Солнечная 3, e-mail: sergej.kolesnik@gmail.com).

▪ ПРОГНОЗУВАННЯ ТА МОДЕЛЮВАННЯ ЕКОНОМІЧНИХ ПРОЦЕСІВ

UDK 351.863:330.46
DOI: 10.37128/2411-4413-2020-1-6

MANAGEMENT OF INFORMATION RISKS OF THE ENTERPRISE IN THE CONDITIONS OF DIGITALIZATION[6]

YURCHUK Natalia,
Candidate of Economic Sciences,
Associate Professor of
the Department of Computer
Science and Economic Cybernetics,
Vinnytsia National Agrarian University
(Vinnytsia)

The features of modern information risk management are considered and analyzed in the article. The influence of digitalization of enterprises on information security is analyzed.

Approaches to the interpretation of the definition of "information risk" are analyzed. It is indicated that information risks arise primarily from the creation, transmission, storage, processing, use of information in practical activities using digital media and other information and communication means. The purpose of risk management of information risks of the enterprise is to minimize the costs of counteracting information risks and the overall losses from them. Information risks include risks of internal and external fraud, unauthorized use of company resources, breach of confidentiality, integrity and reliability of information, etc.

The proposed information risk management system provides for the implementation of such procedures as identification of information risks, analysis of information risks, selection and implementation of the method of reducing information risks, control of information risks.

[6] ***YURCHUK N.P., 2020***

It has been found that it is advisable to use models based on international standards when modeling information threats. Popular practices used in practice are based on standards such as ISO / IEC 27005: 2011, NIST SP800-30, EBIOS, OCTAVE.

It is determined that quantitative calculation of risk situations is used first of all when it is necessary to choose the optimal variant of solving a risk situation. Enterprise information risk management techniques include organizational and technological measures.

It is established that the methods of information risk management of the enterprise include organizational and technological measures. Organizational methods of risk reduction include: risk aversion, loss prevention, loss minimization, transfer of risk control, risk sharing method, information seeking, control or risk management. Technology measures include the accumulation of risk information, their assessment and analysis, ranking and informing management about the implementation of risks and the likelihood of their occurrence, the use of modern data protection systems (obstruction, access control, masking, regulation, etc.).

It is established that the choice of information risk management methodology in each individual case depends on the specific activity of the enterprise.

Keywords: information risks, information risk management system, risk analysis, risk identification, risk map, risk management.

Tab.: 1. Fig.: 2. Lit.: 21.

УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВІЗАЦІЇ

ЮРЧУК Н. П.,
кандидат економічних наук,
доцент кафедри комп'ютерних наук
та економічної кібернетики,
Вінницький національний аграрний університет
(м. Вінниця)

У статті розглянуто та проаналізовано особливості сучасного інформаційного ризик-менеджменту. З'ясовано вплив цифровізації підприємств на інформаційну безпеку.

Проаналізовано підходи до трактування дефініції «інформаційний ризик». Означено, що інформаційні ризики виникають перш за все при створенні, передачі, зберіганні, обробці, використанні інформації в практичній діяльності із застосуванням цифрових носіїв та інших інформаційно-комунікаційних засобів. Метою ризик-менеджменту інформаційних ризиків підприємства є мінімізація витрат на протидію інформаційним ризикам і загальних втрат від них. До інформаційних ризиків можна віднести ризики внутрішнього і зовнішнього шахрайства, несанкціонованого використання ресурсів компанії, порушення конфіденційності, цілісності та достовірності інформації і т.п.

Запропонована система управління інформаційними ризиками передбачає реалізацію таких процедур, як виявлення інформаційних ризиків, аналіз інформаційних ризиків, вибір і реалізація методу зниження інформаційних ризиків, контроль інформаційних ризиків.

Розкрито, що ідентифікація інформаційного ризику передбачає складання переліку елементів ризику та їх опис: об'єкти захисту, загрози, вразливості. Запропоновано класифікацію інформаційних ризиків, яка дозволяє здійснювати подальші процедури управління ризиком.

З'ясовано, що при моделюванні інформаційних загроз доцільно застосовувати моделі,

що ґрунтуються на міжнародних стандартах. Популярні методики, що використовуються у практичній діяльності базуються на таких стандартах, як ISO/IEC 27005:2011, NIST SP800-30, EBIOS, OCTAVE.

Визначено, що кількісний розрахунок ризикових ситуацій використовується перш за все, коли необхідно обрати оптимальний варіант вирішення ризикової ситуації. Методи управління інформаційними ризиками підприємства включають організаційні та технологічні заходи.

Установлено, що методи управління інформаційними ризиками підприємства передбачають організаційні та технологічні заходи. До організаційних методів зниження ризику відносять: відхилення ризику, недопущення збитків, мінімізація збитків, передача контролю за ризиком, метод розподілу ризиків, пошук інформації, контроль або опанування ризиком. Технологічні заходи передбачають акумуляцію інформації про ризики, їх оцінку та аналіз, ранжування та інформування керівництва про реалізацію ризиків та ймовірність їх настання, використання сучасних систем захисту даних (перешкода, керування доступом до інформації, маскування, регламентація, тощо).

Встановлено, що вибір методики управління інформаційними ризиками у кожному окремому випадку залежить від специфіки діяльності підприємства.

Ключові слова: інформаційні ризики, система управління інформаційними ризиками, аналіз ризиків, ідентифікація ризиків, карта ризиків, ризик-менеджмент.

Табл.: 1. Рис.: 2. Літ.: 21.

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ ПРЕДПРИЯТИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

ЮРЧУК Н.П.,
кандидат экономических наук,
доцент кафедры компьютерных наук
и экономической кибернетики,
Винницкий национальный аграрный университет
(г. Винница)

В статье рассмотрены и проанализированы особенности современного информационного риск-менеджмента. Определено влияние цифровизации предприятий на информационную безопасность.

Проанализированы подходы к трактовке дефиниции «информационный риск». Отмечено, что информационные риски возникают, прежде всего, при создании, передаче, хранении, обработке, использовании информации в практической деятельности с использованием цифровых носителей и других информационно-коммуникационных средств. Целью риск-менеджмента информационных рисков предприятия является минимизация расходов на противодействие информационным рискам и общих потерь от них.

Предложенная система управления информационными рисками предполагает реализацию таких процедур, как выявление информационных рисков, анализ информационных рисков, выбор и реализация метода снижения информационных рисков, контроль информационных рисков.

Раскрыто, что идентификация информационного риска предусматривает составление перечня элементов риска и их описание: объекты защиты, угрозы, уязвимости. Предложена классификация информационных рисков, которая позволяет осуществлять

дальнейшие процедуры управления риском.

Выяснено, что при моделировании информационных угроз целесообразно применять модели, основанные на международных стандартах. Популярные методики, используемые в практической деятельности, базируются на таких стандартах, как ISO / IEC 27005: 2011, NIST SP800-30, EBIOS, OCTAVE.

Определено, что количественный расчет рисковых ситуаций используется прежде всего, когда необходимо выбрать оптимальный вариант решения рисковой ситуации. Методы управления информационными рисками предприятия включают организационные и технологические мероприятия.

Установлено, что выбор методики управления информационными рисками в каждом отдельном случае зависит от специфики деятельности предприятия.

Ключевые слова: информационные риски, система управления информационными рисками, анализ рисков, идентификация рисков, карта рисков, риск-менеджмент.

Табл .: 1. Рис .: 2. Лит .: 21.

Problem statement. The rapid dynamics of modern life creates new problems, activates methodological searches, forms new paradigms for studying economic processes [1]. Digital transformation of the economy, which is based on progressive digital technologies, plays a paramount role in the dynamic development of the country in the context of integration and globalization processes. The advent of digital technologies creates new opportunities for market players to function in the online space, increasing their competitive and innovative potential by enhancing their productivity, including through rapid scaling and digitization of their activities [2].

The rapid development of enterprise IT infrastructure leads to an uncontrolled increase in the number of information threats and vulnerabilities of information resources. In these conditions, information risk assessment allows to determine the necessary level of information protection, to support it and to develop a strategy for the development of the information structure of the company [3].

The progressive development of the economy, the increasing needs of humanity are fully subordinated to entrepreneurial activity, which is the key to creating opportunities to meet public needs [4].

The rapid pace of computerization of society in all spheres of human activity has led and is leading to the emergence of new and the spread of already known risks and threats. More and more unconventional channels of information gathering, unauthorized access to management information and interference with government networks, military and law enforcement agencies, all other social hierarchies and social institutions, various terrorist and criminal organizations and groups are constantly appearing cyberspace in virtually unlimited, uncontrolled and unpredictable volumes [5].

In the conditions of market environment, significant transformations in economic relations between economic entities, theoretical and practical issues of structural transformation are of particular importance [6].

Of course, the benefits of digital technologies are significant, but their implementation poses a threat to information security for businesses. Continuous growth in the use of digital technologies is increasing the number of information

security breaches. According to the monitoring service of registration data of Ukrainian companies and the court registry for protection against raids and control of counterparties Opendatabot [7], the number of cybercrime in Ukraine has increased at least 2.5 times in the last five years. The number of cybercrimes has jumped in 2017. It is largely related to the «Petya» virus. However, since then the number of information crimes has not decreased. The number of cases brought against cybercriminals is increasing not only because the crimes themselves have increased. The second reason is that there are more professionals able to detect these crimes.

In 2015, 432 cases were opened for hacking into computers, systems or networks and for interfering with (or blocking) their work, in 2016 - 294, and in 2017 - 1795. As for crimes for writing and spreading viruses, then there are two jumps at once: in 2015, there were 21 such cases, in 2016 - 15, in 2017 - 35, in 2018 - 134. The number of crimes for unauthorized acts with electronic information has increased in 2015, 75 cases were opened, in 2016 - already 311, in 2017 - 670, in 2018 – 1070 [7].

Thus, for the normal functioning of the enterprise in terms of digitization, it is necessary to ensure its information security, and, accordingly, information risk management.

Analysis of recent research and publications. In the scientific and practical literature much attention is paid to the study of theoretical and applied aspects of information risk management of the enterprise, in particular such Ukrainian and foreign researchers as: Artishchuk I.V. [8], Honcharuk I.V. [4], Iskadzhian S.O. [9], Kaletnik H.M. [1], Kiselev I.A. [9], Kozlova E.A. [10], Okhrimenko A.O. [3], Fedulova I.V. [11], Chunaryova A.V., Parkhomenko I.I., Sashchuk I.I. [12] and others.

Kislov D.V. [5] explores the problems of occurrence of risks in the processes of information transformations in the structures of state marketing communications and in making and implementing managerial decisions.

Information Security Standard BS ISO / IEC 27005: 2011, which in Ukraine is named DSTU ISO / IEC 27005: 2015 Information Technology. Methods of protection. Information Security Risk Management (ISO / IEC 27005: 2011, IDT) [13], effective in Ukraine at the beginning of 2017.

It provides guidance for information security risk management, which includes information and security risk management for telecommunications technologies.

Improvement of the methodology of information risk assessment in automated systems using basic techniques and requirements of international standards, proving the efficiency of the methodology with the help of a software product, which is a prototype of the expert system proposed in the work of Buchik S.S. and Melnyk S.V. [14].

Research of methods of risk management, development of methodology of analysis and forecasting of financial risks taking into account their information component was made in the work of Kuznetsova N.V. [15].

However, despite increasing attention to enterprise risk management research, systematic research on the issue of information risk management in the context of enterprise digitalization requires.

Goals setting. The purpose of the article is to investigate the features of information risk management in the context of digitization of enterprises from the standpoint of a systematic approach.

Presentation of the main material of the research. Modern scientific publications, regulatory documents highlight various aspects of the concept of "information risk", which differ in the level of detail and concretization of the concept, purpose and objectives of the research.

BS ISO / IEC 27005: 2011 [13] discloses information security risk as a potential use of an asset or group of assets vulnerabilities as a specific threat to cause damage to an organization.

Lipayev V.V. [16] characterizes information risk as a possible event that results in the unauthorized destruction, distortion of information, and breach of its confidentiality or accessibility.

The Regulation on the Organization of Risk Management Systems in Banks of Ukraine and Banking Groups [17] defines information risk as the likelihood of loss or additional loss or loss of planned income as a result of internal and external events regarding the bank's information systems and other information resources used to achieve the goals of the bank, insufficient internal control or inadequate or erroneous internal processes of the bank in the field of information and communication technologies. Information risk is a component of operational risk.

Buchik S.S., Melnik S.V. [14] note that risk is a complex value that is characterized only by identifying a combination of factors such as threats, incidents, vulnerabilities and types of losses. These factors alone do not make it possible to correctly describe the risk and determine its level.

In the work of Kuznetsova N.V. [18], information risks are proposed to mean the threat of loss or damage resulting from the use of information technology and indicate that information risks are closely linked to the creation, transmission, storage and use of information through electronic media or other means of communication.

A.O. Okhrimenko [3] emphasizes that it is possible to distinguish one characteristic of risk, which occurs in all definitions and unites them - an event that must occur, which is related to probability, action or activity, measure, frequency, the choice of certain solutions, uncertainty, loss, danger, etc.

Information risks arise primarily from the creation, transmission, storage, processing, use of information in practical activities using digital media and other information and communication means.

The purpose of the enterprise information risk management is to minimize the costs of counteracting information risks and the overall losses from them. Information risks include risks of internal and external fraud, unauthorized use of company resources, breach of confidentiality, integrity and reliability of information, etc.

In Fig. 1 shows the information risk management system.

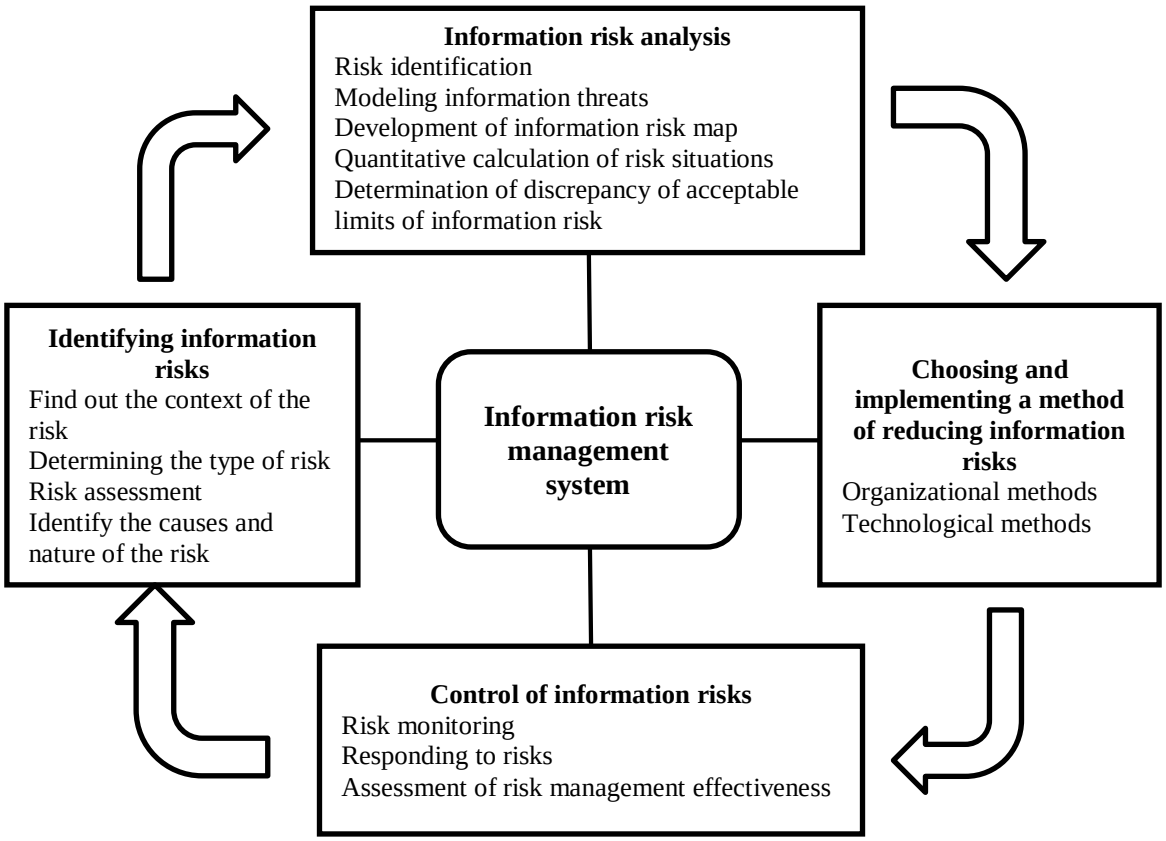

Fig. 1. **The enterprise information risk management system**
Source: developed by the author in [15]

Risk management is the process of identifying, managing, eliminating, or reducing the likelihood of events that may adversely affect the resources of the information system, reducing security risks, potentially having the potential to affect information security, provided the security value is acceptable.

Risk management includes all operations that can be performed on information security risk: minimization (risk reduction), neutralization, risk retention (risk retention), risk transfer or insurance (risk transfer) [3].

Explaining the risk context means identifying internal and external parameters that will be taken into account in managing the risks, as well as defining the scope and risk criteria to reflect in the risk management strategy [19]. Explaining the context of risk is well described by the SWOT matrix. An analysis of the environment and the context of risks enables the company to clearly identify its current status, identify major strategic problems, develop an adequate strategy and analyze the risks that may affect its implementation [11].

Determining the type of information risk allows you to identify the source of the risk situation. The concept of risk is multidimensional, so, depending on the scope and stages of the hazard analysis, different types of information risk are identified (Table 1).

The classification of information risks allows for further risk management procedures.

Table 1

Classification of information risks of the enterprise

Classification feature	Types of information risks
By sphere of influence	- external, occurring outside the information system of the enterprise in the course of its normal functioning; - internal, occurring inside the enterprise information system due to the loss or disruption of interconnections of individual subsystems;
By the nature of occurrence	- intentional influence of employees of the enterprise, as well as of third parties; - accidental influence that arises regardless of time and place, as well as the will of the participants of the process;
By sources of risk	- anthropogenic caused by human or group actions; - man-made, caused by technical failures, accidents and catastrophes; - natural climatic conditions caused by climatic negative impacts;
By risk size	- maximum (catastrophic), which cause a significant amount of damage to the enterprise information system or its subsystems; - medium (significant), causing an average amount of damage to the enterprise information system or its subsystems; - weak (insignificant), which do not cause or cause a small amount of damage to the enterprise information system or its subsystems
Duration of exposure	- temporary (short-term) - within a few seconds or hours; - permanent (long-term) - for days, months and years;
By frequency of exposure	- disposable, non-repetitive; - recurrent, recurring over a period of time;
By type of influence	- resources when there are problems in logistical support, technical defects, moral backwardness and incompatibility of technical, software, etc.; - technological, caused by non-observance of production technology and non-configurability of information system technology; - network software caused by network and software defects, virus penetration, etc .;
Originally	- related to loss of information; - related to the formation of an information resource; - related to information influence on the activity of enterprises;
By form of influence	- quantitative; - qualitative.

Source: summarized by the author based on [3; 5; 9]

Identification of information risk involves the compilation of a list of risk elements and their description: objects of protection, threats, vulnerabilities. Security assets include information assets, intangible assets, including Software; hardware, network equipment, people, reputation and image of the enterprise. The practice of identifying information risk is assessed by the first four groups.

The baseline data for identifying threats and vulnerabilities may be information about information security incidents, audit findings, expert assessments of users, information security professionals, IT professionals.

The output information at this stage is used to calculate the amount of risk or potential loss that an enterprise will receive in the event of an information security breach or the likelihood of such a breach. It also determines the severity of the consequences of a violation of integrity, accessibility, and confidentiality.

When modeling information threats, it is advisable to use models based on international standards. Popular practices used in practice are based on standards such as ISO / IEC 27005: 2011, NIST SP800-30, EBIOS, OCTAVE.

One of the main stages of risk analysis should be the modeling of information threats. Information threats modeling allows to determine the probable consequences

of information risks impact on the activity of the enterprise, to estimate available resources, to analyze the cause and effect relationships between threats, to identify the weakest areas exposed to external information threats.

Based on the results of the initial data assessment, a risk map can be prepared, presented in the form of a graphical and textual description of certain types of risks presented in the form of a rectangular table. On one coordinate axis the significance of risk is indicated, on the other - the probability or frequency of its occurrence (Fig. 2) [8].

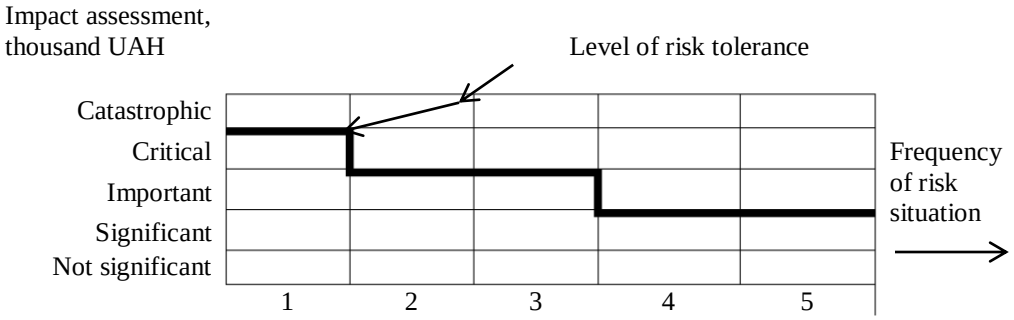

Fig. 2. **Example of risk map and tolerance limits**

Source: [18]

The risk map is constructed on the basis of the following parameters: probability of risk action (occurrence of risk situations); the proportion of the magnitude of the losses incurred as a result of the risk in relation to the planned profit for the period. To build a risk map, the limits of risk tolerance (Fig. 2) of a particular species are distinguished. Risk tolerance is the permissible level at which an entity maintains financial sustainability. It consists of a set of subjective and objective factors that shape risk situations. Subjective factors include those related to personalization of decision making. This can already be a problem, since the decision is always made by a particular person (manager) and people are notoriously at risk. It follows that the level of tolerance is determined by the human characteristics of the decision-maker (group of persons) [8].

Quantitative calculation of risk situations is used first of all when it is necessary to choose the optimal variant of solution of risk situation. The use of quantitative risk assessment methods is based on systematic analysis and design methods.

In practice, quantitative methods allow:

- automatically classify information risks;
- quickly formulate information risk models based on asset security;
- Risk ranking (threat level: very high, high, medium, low, very low, vulnerability level: high, medium, low, none);
- to argue the cost of ensuring information security of the company;
- formalize and automate risk assessment and management procedures [9].

The most well-known approach to quantitative information risk calculation is the British CRAMM method. Its main goals are: automation of information risk management, optimization of financial expenses for management, optimization of time

for maintenance of company security systems, support of business continuity, etc. [9].

Conditionally, risk analysis can be divided into several groups. The first is the development of scientific methods of risk analysis based on known theories and requirements of standards for the creation of an information security management system. The second group includes specialized software products, which are usually based on the methods of the first group, but are more practical and take better account of the specifics of the object of protection. Let's analyze the first group. Scientific methods of risk analysis use different sections of higher mathematics: set theory, probability theory, and discrete mathematics. Principles based on reliability theory and fuzzy set theory are chosen as the core of the approaches. A feature of risk assessment is the complexity of formalizing the task and obtaining quantitative estimates. One method of assessing information security risks based on the determination of optimal values is a method based on the calculation of mutual information and the application of the so-called K-means clustering algorithms [10].

The method determines the degree of quantitative relationship between risk factors and the level of information security with the calculation of mutual information. At each risk level, the K-means algorithm determines the optimal points as the initial centers of the clusters, and then the K-means clustering algorithm classifies the data. The method can dynamically adjust the center of the cluster according to the results of the clustering and calculation of mutual information values. This method is easy to apply it has fewer calculations than other methods. The method is less sensitive to the input data.

The second group of approaches to risk assessment is more developed by foreign authors. Authors from the USA, England are primarily advisory in improving the already existing standards of information security: ISO, BS and do not require a deep knowledge of higher mathematics.

In many cases, the third group of approaches combines expert and risk assessments based on the determination of their likelihood based on available statistics. Such approaches can be successfully applied in practice, as the use of statistics base allows to minimize the subjective view of the expert on the task and to carry out work on the assessment of information security risks to specialists without extensive experience and qualifications. To solve this problem, a number of software complexes for information risk analysis and control were developed, the main ones being: British CRAMM (Insight Consulting), American Risk Watch (Risk Watch) and Russian GRIF (Digital Security Company) [12].

Based on the analysis, it is possible to determine the contingent limits of information risks, calculated by the formula:

$$R = P_{threats} R_n C \frac{K_o + K_t}{2} 100\%, \quad (1)$$

where R – is the numerical value of the risk of information security threats; $P_{threats}$ – the likelihood of the implementation of at least one threat from the entire list of actual threats; R_n – risk of non-compliance with legal requirements; C – the value of

the asset; K_o – probability of exploitation of organizational vulnerabilities; K_t – probability of exploitation of technical vulnerabilities [9].

Methods of information risk management of the enterprise include organizational and technological measures.

Organizational methods of risk reduction include: risk aversion, loss prevention, loss minimization, transfer of risk control, risk sharing method, information seeking, control or risk management. Risk rejection implies the rejection of certain management decisions if the risk level for them exceeds its acceptable level for the enterprise. Non-loss assumption implies that an entity may attempt to reduce but not eliminate specific losses. A method of minimizing losses is that an entity may attempt to prevent a significant portion of its losses. Transfer of risk control is done through contracting. The risk-sharing method is that the risk of probable harm or loss is distributed among the participants so that the potential loss of each is small [20].

Technology measures include the accumulation of risk information, their assessment and analysis, ranking and informing management about the implementation of risks and the likelihood of their occurrence, the use of modern data protection systems (obstruction, access control, masking, regulation, etc.).

According to A.V. Denusenko [21] risk control is a phenomenon whose necessity is based on the fact that: 1) the introduction of control will allow to gather information about risks and their signals, which will further ensure prompt response to them; 2) the implementation of controls, which require the implementation of certain actions, aimed at minimizing the likelihood of occurrence of risky events. This conclusion was drawn in view of the specificity of risks as an object of control. That is, the purpose of risk control is to prevent their negative consequences, to minimize the risks of an entity's activities.

The essence of enterprise control, using the subject of control as a key feature, it is advisable to define as:

1) control of the leader, which is expressed in the solution of the problem of establishing compliance of the implementation of management decisions with certain principles, goals, objectives and goals; this level of risk control should be aimed at detecting deviations in the conduct of business transactions and their reflection in the accounting and reporting entity;

2) control exercised by each participant of the economic process at the enterprise (expressed in actions of a controlling nature);

3) risk control as an element of information support of management decisions. To determine the essence of the first element of control, we propose to consider it as a dualistic system, due to the need to control the accounting process and the compliance of the employees of the entity.

In order to maximize the effectiveness of this type of control, the frequency of its implementation should be sporadic. The second element of control is systematic. That is, it must be carried out continuously, become a supporting element of all processes that occur in the enterprise during its operation. The third element is related to the organization and maintenance of the information security system and the

functioning of the system of risk identification and assessment as a threat to the activity of the tourism enterprise. Such an element of control should be carried out periodically, depending on the needs of users of information. It is this element that should be considered as risk control, as it will identify the potential threats and the likelihood of occurrence of risk events. Effectiveness of risk control at enterprises will be possible only if the three above defined elements are synthesized [21].

The choice of information risk management methodology in each case depends on the specific activity of the enterprise:

- the degree of dependence of the activity of the enterprise on information technology, importance for the normal functioning of information risks;
- the need for in-depth study of information risks and the ability to carry out risk assessments and identify baselines for reducing information risks;
- availability of human, financial and time resources for implementation of risk management system, including information;
- requirements of legislation, regulators and other stakeholders to the process of information risk management.

Taking into account all the requirements will facilitate the optimal choice of information risk management methodology.

Conclusions. In the context of digital transformation, the role of information has significantly increased. The use of information as a resource contributing to business efficiency has led to information risks that, along with other types of risks, may affect the activities and further development of the enterprise. Information risks arise primarily from the creation, transmission, storage, processing, use of information in the practical activity of the enterprise using digital media and other information and communication means. Information risk management is a subjective, complex and very important process in the activity of enterprises, in particular those who work with large volumes of data, confidential information, for which there is a high probability of leakage, damage, information, software, hardware, networking.

The system of information risk management of the enterprise involves the implementation of procedures such as identification of information risks, analysis of information risks, the choice and implementation of the method of reducing information risks, control of information risks. In order to effectively manage information risks, the methodology chosen must: meet the specifics of the enterprise, take into account available resources, simulate the real situation taking into account all information risks of the enterprise, and take into account the requirements of regulators, management of the enterprise, other stakeholders.

Список використаних джерел

1. Калетнік Г., Козловський С., Козловський В. Стійкість економіки як фактор безпеки та розвитку держави. *Економіка України.* 2012. № 7. С. 16-25.
2. Наторіна А. О. Домінанти цифрової трансформації економіки країни. *Науковий вісник Полтавського університету економіки і торгівлі. Серія: Економічні науки*. 2017. № 5. С. 146-151.

3. Охріменко А.О. Визначення понять ризик і управління ризиками в сфері інформаційної безпеки. *Системи обробки інформації*. 2011. № 7(97). С. 133-134.

4. Гончарук І. В. Аспекти сутності й оцінки ефективності аграрної підприємницької діяльності. *Агроінком.* 2013. № 7-9. С. 100-103.

5. Кіслов Д. В. Інформаційні ризики управлінських систем. Молодий вчений. 2015. № 7(2). С. 144-147.

6. Коляденко С. В. Структурна трансформація в господарських комплексах АПК регіону. *Збірник наукових праць ВНАУ. Серія: Економічні науки.* 2011. № 2 (53), т. 3. С. 181-187.

7. Сайт Opendatabot. Сервіс моніторингу реєстраційних даних та судового реєстру для захисту активів. URL: https://opendatabot.ua/.

8. Артищук І. В. Підходи до побудови карти ризиків на основі врахування впливу базових факторів на діяльність торговельного підприємства. *Торгівля, комерція, підприємництво : збірник наукових праць.* 2011. Вип. 13. С.101-107.

9. Киселева И.А., Искаджян С.О. Управление информационными рисками в бизнесе. *Иннов: электронный научный журнал*, 2017. №1 (30). URL: http://www.innov.ru/science/economy/upravlenie-informatsionnymi-riskami/.

10. Козлова Е.А. Оценка рисков информационной безопасности с помощью метода нечеткой кластеризации и вычисления взаимной информации. *Молодой учёный.* 2013. №5. С. 154-161.

11. Федулова І.В. Стратегія ризик-менеджменту. *Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку*. 2019. Вип. 1. №1. С.65-74.

12. Чунарьова А.В., Пархоменко І.І., Сащук І.І. Аналіз підходів та програмних рішень оцінки і контролю інформаційних ризиків в комп'ютеризованих системах. *Вісник Інженерної академії України*. 2014. Вип. 2. С. 138-142.

13. ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT). URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66912.

14. Бучик С.С., Мельник С.В. Методика оцінювання інформаційних ризиків в автоматизованій системі. *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць.* Житомир: ЖВІ ДУТ, 2015. Вип. 11. С. 33-43.

15. Кузнєцова Н.В. Фінансовий ризик-менеджмент з урахуванням інформаційних ризиків. *Реєстрація, зберігання і обробка даних*. 2018. Т.20. №1. С. 30-39.

16. Липаев В. В. Функциональная безопасность программных средств. М.: СИНТЕГ, 2004. 348 с.

17. Положення про організацію системи управління ризиками в банках України та банківських групах. Постанова Правління Національного банку

України 11.06.2018. № 64. URL: https://zakon.rada.gov.ua/laws/show/v0064500-18/ed20180611#n34.

18. Кузнєцова Н.В. Деякі аспекти мінімізації інформаційних ризиків у банківській діяльності. *Системні дослідження та інформаційні технології*. 2014. № 1. С. 7-19.

19. ISO/IEC GUIDE 73:2002. Risk management-Vocabulary – Guidelines for use in standards. International Organization for Standardization, 2002. URL: https://www.iso.org/standard/34998.html.

20. Корецька О.В. Методи зниження ризиків як засіб забезпечення конкурентоспроможності підприємств. URL: https://www.kpi.kharkov.ua/archive/MicroCAD/2016/S23/s256.pdf.

21. Денисенко А.В. Роль та місце контролю в процесі управління ризиками на туристичних підприємствах. *Економіка і регіон.* 2014. № 2. С. 81-85.

References

1. Kaletnik H., Kozlovs'kyj S. & Kozlovs'kyj V. (2012) Stijkist' ekonomiky iak faktor bezpeky ta rozvytku derzhavy [Economic stability is a factor of security and development of the state]. *Ekonomika Ukrainy – Economy of Ukraine*, 7. pp. 16-25 [in Ukrainian].

2. Natorina A.O. (2017) Dominanty tsyfrovoi transformatsii ekonomiky krainy [Digital transformation dominants of the of the country's economy]. *Naukovyj visnyk Poltavs'koho universytetu ekonomiky i torhivli. Seriia : Ekonomichni nauky – Scientific Bulletin of Poltava University of Economics and Trade. Series: Economic Sciences*. 5. pp. 146-151 [in Ukrainian].

3. Okhrimenko A.O. (2011) Vyznachennia poniat' ryzyk i upravlinnia ryzykamy v sferi informatsijnoi bezpeky [Definition of risk concepts and risk management in information security]. *Systemy obrobky informatsii – Information processing systems*, 7 (97). pp. 133-134 [in Ukrainian].

4. Honcharuk I.V. (2013) Aspekty sutnosti j otsinky efektyvnosti ahrarnoi pidpryiemnyts'koi diial'nosti [Aspekty sutnosti j otsinky efektyvnosti ahrarnoi pidpryiemnyts'koi diial'nosti]. *Ahroinkom – Ahroinkom*. 7-9. pp. 100-103 [in Ukrainian].

5. Kislov D.V. (2015) Informatsijni ryzyky upravlins'kykh system. [Information risk of management systems]. *Molodyj vchenyj – Young Scientist*, 7(2), pp. 144-147 [in Ukrainian].

6. Koliadenko S.V. (2011) Strukturna transformatsiia v hospodars'kykh kompleksakh APK rehionu [Structural transformation of economic systems of agriculture in the region]. *Zbirnyk naukovykh prats' VNAU. Seriia: Ekonomichni nauky – Collection of scientific works of VNAU. Series: Economic Sciences*. 2 (53). Vol. 3. pp. 181-187 [in Ukrainian].

7. Sajt Opendatabot. Servis monitorynhu reiestratsijnykh danykh ta sudovoho reiestru dlia zakhystu aktyviv [Registration and court monitoring service for asset protection]. Retrieved from https://opendatabot.ua/ [in Ukrainian].

8. Artyschuk I.V. (2011) Pidkhody do pobudovy karty ryzykiv na osnovi vrakhuvannia vplyvu bazovykh faktoriv na diial'nist' torhovel'noho pidpryiemstva [Approacher to the construction of maps based on risk of incorporation of factors for trading enterprises]. *Torhivlia, komertsiia, pidpryiemnytstvo: zbirnyk naukovykh prats' – Trade, commerce, entrepreneurship: a collection of scientific works*. Vol. 13. pp. 101-107 [in Ukrainian].

9. Kiseleva I.A. & Iskadzhjan S.O. (2017) Upravlenie informacionnymi riskami v biznese [Information risk management in business]. *Innov: jelektronnyj nauchnyj zhurnal – Innov: an electronic scientific journal*, 1 (30). Retrieved from http://www.innov.ru/science/economy/upravlenie-informatsionnymi-riskami/ [in Russian].

10. Kozlova E.A. (2013) Ocenka riskov informacionnoj bezopasnosti s pomoshh'ju metoda nechetkoj klasterizacii i vychislenija vzaimnoj informacii [Assessing information security risks using the fuzzy clustering method and the calculation of mutual information]. *Molodoj uchjonyj – Young scientist*. 5. pp. 154-161. Retrieved from https://moluch.ru/archive/52/6967/ [in Russian].

11. Fedulova I.V. (2019) Stratehiia ryzyk-menedzhmentu [Risk management strategy]. *Menedzhment ta pidpryiemnytstvo v Ukraini: etapy stanovlennia i problemy rozvytku – Management and Entrepreneurship in Ukraine: Stages of Formation and Problems of Development*. Vol. 1. pp. 65-74 [in Ukrainian].

12. Chunar'ova A.V., Parkhomenko I.I. & Saschuk I.I. (2014) Analiz pidkhodiv ta prohramnykh rishen' otsinky i kontroliu informatsijnykh ryzykiv v komp'iuteryzovanykh systemakh [Analysis of approaches and software solutions for information risk assessment and control in computer systems]. *Visnyk Inzhenernoi akademii Ukrainy – Bulletin of engineering academy of Ukraine*, Vol. 2, pp. 138-142 [in Ukrainian].

13. DSTU ISO/IEC 27005:2015 Informatsijni tekhnolohii. Metody zakhystu. Upravlinnia ryzykamy informatsijnoi bezpeky [DSTU ISO / IEC 27005: 2015 Information technology. Methods of protection. Information security risk management]. Retrieved from http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66912 [in Ukrainian].

14. Buchyk S.S. & Mel'nyk S.V. (2015) Metodyka otsiniuvannia informatsijnykh ryzykiv v avtomatyzovanij systemi [Methods of estimation of informative risks in automated system]. *Problemy stvorennia, vyprobuvannia, zastosuvannia ta ekspluatatsii skladnykh informatsijnykh system: zbirnyk naukovykh prats' – Problems of creation, testing, application and operation of complex information systems: a collection of scientific works*. Vol. 11. pp. 33-43 [in Ukrainian].

15. Kuznietsova N.V. (2018) Finansovyj ryzyk-menedzhment z urakhuvanniam informatsijnykh ryzykiv [Financial risk management based on information risks]. *Reiestratsiia, zberihannia i obrobka danykh – Registration, storage and processing of data*. Vol. 1, pp. 30-39 [in Ukrainian].

16. Lipaev V.V. (2004) Funkcional'naja bezopasnost' programmnyh sredstv [Functional safety of software]. M.: SINTEG 348 p. [in Russian].

17. Polozhennia pro orhanizatsiiu systemy upravlinnia ryzykamy v bankakh Ukrainy ta bankivs'kykh hrupakh. Postanova Pravlinnia Natsional'noho banku Ukrainy 11.06.2018. 64. Retrieved from https://zakon.rada.gov.ua/laws/show/v0064500-18/ed20180611#n34 [in Ukrainian].

18. Kuznietsova N.V. (2014) Deiaki aspekty minimizatsii informatsijnykh ryzykiv u bankivs'kij diial'nosti [Some aspects of minimizing information risks in banking]. *Systemni doslidzhennia ta informatsijni tekhnolohii – System research & information technologies.* 1. pp. 7-19 [in Ukrainian].

19. ISO/IEC GUIDE 73:2002. Risk management-Vocabulary – Guidelines for use in standards. International Organization for Standardization (2002). Retrieved from https://www.iso.org/standard/34998.html [in Switzerland].

20. Korets'ka O.V. (2016) Metody znyzhennia ryzykiv iak zasib zabezpechennia konkurentospromozhnosti pidpryiemstv [Risk mitigation methods as a means of ensuring the competitiveness of enterprises]. Retrieved from: https://www.kpi.kharkov.ua/archive/MicroCAD/2016/S23/s256.pdf **[**in Ukrainian].

21. Denysenko A.V. (2014) Rol' ta mistse kontroliu v protsesi upravlinnia ryzykamy na turystychnykh pidpryiemstvakh [Role of control in risk management in the travel companies]. *Ekonomika i rehion – Economy and region.* 2, pp. 81-85 **[**in Ukrainian].

Відомості про автора

ЮРЧУК Наталія Петрівна – кандидат економічних наук, доцент кафедри комп'ютерних наук та економічної кібернетики, Вінницький національний аграрний університет (21008, м. Вінниця, вул. Сонячна, 3, e-mail: urnata@vsau.vin.ua).

YURCHUK Natalia – Candidate of Economic Sciences, Associate Professor of the Department of Computer Science and Economic Cybernetics, Vinnytsia National Agrarian University (21008, 3 Sonyachna st, Vinnytsia, e-mail: urnata@vsau.vin.ua).

ЮРЧУК Наталия Петровна – кандидат экономических наук, доцент кафедры компьютерных наук и экономической кибернетики, Винницкий национальный аграрный университет (21008, г. Винница, ул. Солнечная, 3, e-mail: urnata@vsau.vin.ua).