Облік і оподаткування

УДК 005.334:658.15]:004.9

Ovcharyk Roman

PhD in Economic, Associate Professor,

Associate Professor of the Department of Financial Analysis and Audit

State University of Trade and Economics

Овчарик Роман Юрійович

кандидат економічних наук, доцент,

доцент кафедри фінансового аналізу та аудиту

Державний торговельно-економічний університет

ORCID: 0000-0001-6536-9712

Kopotiienko Tetiana

PhD in Economics, Associate Professor,

Associate Professor of the Department of Financial Analysis and Audit

State University of Trade and Economics

Копотієнко Тетяна Юріївна

кандидат економічних наук, доцент, доцент кафедри

фінансового аналізу та аудиту

Державний торговельно-економічний університет

ORCID: 0000-0001-6107-9937

Mikityuck Ihor

PhD in Economic, Associate Professor,

Associate Professor of the Department of Financial Analysis and Audit

State University of Trade and Economics

Микитюк Ігор Сергійович

кандидат економічних наук, доцент,

доцент кафедри фінансового аналізу та аудиту

Державний торговельно-економічний університет

ORCID: 0000-0001-5523-0485

Kovalenko Dmytro
PhD in Economic, Associate Professor,
Associate Professor of the Department of Management
Kyiv National University of Technologies and Design
Коваленко Дмитро Іванович
кандидат економічних наук, доцент,
доцент кафедри менеджменту
Київський національний університет технологій та дизайну
ORCID: 0000-0002-0853-0546

RISK ANALYSIS AND AUDIT IT-COMPANIES IN THE SYSTEM CONTROL OF THE STABILITY OF THEIR DEVELOPMENT
АНАЛІЗ ТА АУДИТ РИЗИКІВ ІТ-КОМПАНІЙ В СИСТЕМІ КОНТРОЛЮ СТАБІЛЬНОСТІ ЇХ РОЗВИТКУ

Summary. *Introduction. IT companies, carrying out their own economic activity, constantly face numerous threats, which differ significantly in the place and time of appearance, a set of internal and external factors affecting their intensity. This, in turn, determines the methods of analysis and forms approaches to the application of effective management methods. In many cases, threats are interrelated, which can both exacerbate risks and create prerequisites for mitigating them. This nature of interaction makes the decision-making process for risk optimization more comprehensive, requiring a thorough and comprehensive analysis of the causes and prerequisites for the occurrence of various types of hazards. Each threat, regardless of its source, potentially becomes the basis for the formation of a certain risk. Within productive risk management, such threats are often classified into defined categories to make their analysis more systematic and meaningful. The effectiveness of risk management in IT companies directly depends on the correct classification and structuring of risks, which provides a basis for the implementation of effective methods and strategies for minimizing*

potential hazards. In order to get the most accurate picture of the situation, the IT company must identify the most important risk factors, conduct their in-depth analysis and audit. This allows not only to assess the potential impact of threats, but also to find optimal ways to manage business processes, increasing the overall efficiency of activities. Owners and managers of such companies need to take into account both the positive aspects of risk – the possibility of using it in the context of entrepreneurial activity (including its definition, classification and management of prospects), and the negative aspects expressed in the implementation of threats and losses. As a result, competent risk analysis and audit become key elements of a successful strategy for the development of an IT company, contributing to the elimination or significant reduction of the most common threats. It also ensures rapid adaptation to changing circumstances and effective use of opportunities to minimize the impact of dangerous factors on business.

Purpose. Research on key aspects of risk analysis and audit of IT companies, determination of the impact of these risks on the activities of economic entities, as well as development of a system of administrative measures for effective control and reduction of risks to an acceptable level.

Materials and methods. The research materials are: (a) the legal framework governing the activities of economic entities, in particular IT companies, as well as statistical data on their functioning; (b) scientific works by both Ukrainian and foreign authors investigating the issue of risk formation, in particular those specific to the field of IT companies. Research methods are: theoretical generalization and classification, methods of formalization, analysis and synthesis, as well as logical generalization of the obtained results with the formulation of conclusions.

Results. The classification of risk audits for enterprises is presented IT - spheres by type. The main types of risks are identified and analyzed IT - companies, their analysis was carried out. The authors researched and formed

the main tasks of risk analysis and audit IT - companies. According to actual data, the formation of risks was investigated with the help of coefficient analysis IT - companies under the influence of personnel potential factors. In particular, researchers established a connection between the structural changes of technical specialists under the influence of martial law.

Prospects. focus attention on a detailed quantitative analysis of risks arising in IT companies, as well as on the study of the relationship between the level of risk and the financial indicators of their activity. The use of regression-correlation analysis is a promising tool that will contribute not only to the identification of the optimal level of acceptable risk, but also to the justification of measures for its systematic monitoring and control at the management level of the company. The implementation of this approach will enable the heads of IT companies to more effectively manage risks, promptly respond to emerging problems and threats, which will contribute to increasing the overall productivity of the organization and achieving optimal results of its work.

Key words: *risk, IT-companies, risk analysis, risk audit, risk control, HR risk, economic security, financial security, financial analysis, strategic analysis, cybersecurity.*

Анотація. *Вступ. ІТ-компанії, здійснюючи власну господарську діяльність, постійно стикаються з численними погрозами, які значно відрізняються за місцем і часом появи, сукупністю внутрішніх і зовнішніх факторів, що впливають на їхню інтенсивність. Це у свою чергу визначає способи проведення аналізу і формує підходи до застосування ефективних методів управління. У багатьох випадках загрози взаємопов'язані, що може як посилювати ризики, так і створювати передумови для їх пом'якшення. Такий характер взаємодії робить процес ухвалення рішень щодо оптимізації ризиків більш комплексним, вимагаючи ретельного і всебічного аналізу причин та передумов виникнення різних типів небезпек. Кожна загроза, незалежно від її джерела, потенційно стає підґрунтям для*

формування певного ризику. У межах продуктивного управління ризиками такі загрози часто класифікують за визначеними категоріями, щоб зробити їх аналіз більш системним і осмисленим. Ефективність управління ризиками в IT-компаніях безпосередньо залежить від правильності класифікації та структуризації ризиків, що забезпечує основу для впровадження дієвих методів і стратегій мінімізації потенційних небезпек. Щоб отримати максимально точну картину ситуації, IT-компанія повинна виділити найважливіші фактори ризику, провести їх глибокий аналіз і аудит. Це дозволяє не лише оцінити потенційний вплив загроз, але й знайти оптимальні шляхи управління бізнес-процесами, підвищуючи загальну ефективність діяльності. Власникам і керівникам таких компаній необхідно враховувати як позитивні аспекти ризику – можливість використання його у контексті підприємницької діяльності (включаючи його визначення, класифікацію та управління перспективами), так і негативні сторони, що виражаються у реалізації загроз і втрат. У результаті грамотний аналіз і аудит ризиків стають ключовими елементами успішної стратегії розвитку IT-компанії, сприяючи ліквідації або значному скороченню найбільш поширених загроз. Це також забезпечує швидку адаптацію до змін обставин та ефективне використання можливостей для мінімізації впливу небезпечних факторів на бізнес.

Мета. Дослідження ключових аспектів аналізу та аудиту ризиків IT-компаній, визначення впливу цих ризиків на діяльність суб'єктів господарювання, а також розробка системи адміністративних заходів для ефективного контролю і зведення ризиків до прийнятного рівня.

Матеріали і методи. Матеріалами дослідження є: а) нормативно-правову базу, що регулює діяльність суб'єктів господарювання, зокрема IT-компаній, а також статистичні дані про їх функціонування; б) наукові праці як українських, так і зарубіжних авторів, які досліджують питання формування ризиків, зокрема специфічних до сфери IT-компаній. Методами

дослідження є: теоретичне узагальнення та класифікація, методи формалізації, аналізу і синтезу, а також логічне узагальнення отриманих результатів із формулюванням висновків.

Результати. Представлено класифікацію аудитів ризиків для підприємств IT-сфери за видами. Визначено та проаналізовано основні види ризиків IT-компаній, проведено їх аналіз. Автори дослідили і сформували основні завдання аналізу та аудиту ризиків IT-компаній. За фактичними даними з допомогою коефіцієнтного аналізу досліджено формування ризиків IT-компаній під впливом факторів кадрового потенціалу. Зокрема дослідники встановили зв'язок між структурними змінами технічних спеціалістів під впливом воєнного стану.

Перспективи. зосередити увагу на детальному кількісному аналізі ризиків, що виникають в IT-компаніях, а також на вивченні взаємозв'язку між рівнем ризику та фінансовими показниками їхньої діяльності. Використання регресійно-кореляційного аналізу є перспективним інструментом, який сприятиме не лише ідентифікації оптимального рівня прийнятного ризику, але й обґрунтуванню заходів для його систематичного моніторингу та контролю на управлінському рівні компанії. Реалізація такого підходу дасть змогу керівникам IT-компаній більш ефективно управляти ризиками, оперативно реагувати на виникаючі проблеми та загрози, що сприятиме підвищенню загальної продуктивності організації й досягненню оптимальних результатів її роботи.

Ключові слова: *ризик, IT-компанії, аналіз ризику, аудит ризику, контроль ризику, кадровий ризик, економічна безпека, фінансова безпека, фінансовий аналіз, стратегічний аналіз, кібербезпека.*

Problem statement. Negative economic trends, global instability and rapid development of technologies have created conditions under which IT companies have found themselves under unprecedented pressure of various risks. To respond

to new challenges, many of them are rapidly implementing analysis and control systems aimed at managing the situation more effectively. However, in order to fully counter threats, the supervisory boards and management of such companies need a comprehensive strategic approach that will allow not only to adequately assess future risks, but also to act preventively, instead of reacting retroactively. In doing so, particular attention should be paid to prioritizing compliance requirements. Risk should serve as a strategic tool for improving efficiency and creating business added value. With growing attention to transparency and accuracy of financial reporting, regulatory compliance and building a solid foundation for the company's financial well-being, IT managers are increasingly directing efforts to improve the analysis and control system, as well as risk management, seeking to maximize the benefits of risk audit functions. This highlights the need to rethink and adapt existing approaches to risk management in IT companies to ensure effective management in the face of growing uncertainty.

Analysis of recent research and publications. The work of a number of well-known domestic scientists, among whom we can single out such authors as: Baldyniuk V. [11], Bezverkhyi K. [12], Chyzh L.P.[5], Defir I.V. [13], Dergacheva V.V. [4], Drabenko T. [14], Gordopolov V.Y. [12], Hrytsai O.I. [13], Khotieieva N.V. [5], Koretska O.V. [5], Kotvytska N.M. [15], Kozak O.I. [13], Kryvda O. [6, 14], Kucher A. [8], Kuzminska N. [14], Levkov K. [8], Matiyash D.O. [4], Moyseyenko O. [8], Mysiuk V. [8], Nazarova K.O. [7, 8], Nezhyva M. [8], Ocheretiana O. [6], Oherchuk Y.V. [10], Ostapets A. O. [16], Ovsiienko N.V. [15], Ovsiienko V.V. [15], Parasiy-Vergunenko I.M. [12; 16], Sytnyk N.V. [9], Sytnyk V.F. [9], Tomashkov S. B. [10] and others. Researchers in the field of science apply a variety of approaches to IT risk analysis and management methods, developing assessment tools and implementing control mechanisms to minimize their impact.

In the context of research on risks in business activities, scientists N. Kuzminska, O. Kryvda and N. Drabinko emphasize the significance of qualitative analysis, which is mainly based on a subjective assessment of the key characteristics of risk, its impact on the functioning of the enterprise and the probability of implementation. Such a methodological approach to risk assessment is especially relevant in situations where it is necessary to quickly carry out a preliminary analysis, but the availability of quantitative data turns out to be limited. Quantitative risk analysis, based exclusively on mathematical and statistical data, provides a more detailed treatment of threats through modeling risk scenarios, researching the distribution of probabilities and assessing the sensitivity of various influencing factors. The application of a comprehensive approach to analysis allows you to create a comprehensive idea of the multidimensional nature of the risks inherent in the company's activities in a specific time period. This covers both a general overview and an in-depth treatment of certain features of risks. Even within the framework of qualitative analysis, enterprises can obtain important information on potential threats, which includes identifying risk areas, predicting possible adverse effects or additional benefits. Based on the obtained conclusions, the management of the organization is able to make rationally based decisions regarding the strategic directions of further development [6; 14].

Economists Nataliya Ovsienko, Nataliya Kotvytska and Volodymyr Ovsienko focus the attention of specialists in the field of risk management on the importance of the risk identification process. This process involves identifying potential threats or opportunities that can affect the success of a project both negatively and positively. The Project Management Institute (PMI) methodology offers a wide range of tools for collecting and analyzing information within risk identification, including the «brainstorming method, source analysis, SWOT analysis, and peer reviews. The result of this stage is the creation of a risk register. Qualitative risk analysis – is the next step after identification aimed at determining

the details of each of its factors. It includes an assessment of the probability of its appearance and possible consequences. The main advantage of this process is to reduce the level of uncertainty of the project manager and focus efforts on the highest priority risks that require attention and management [15].

Vasyl Baldynyuk, a researcher from Vinnytsia, emphasizes that ensuring the success and financial stability of the enterprise under modern conditions is possible only under the condition of a thorough analysis of the situation and competent risk management. In this regard, managers and specialists in the field of risk management must be fully informed about the factors of risk occurrence and their probability levels during the implementation and operation of the risk management system. In addition, particular attention should be paid to clearly distinguishing between the objects and the entities involved in the risk management process [11]. We want to supplement – with this possible only if the analysis and audit are carried out in a timely manner e risks in IT -companies with a view to further monitoring their level.

Within the domestic scientific space, considerable attention is paid to the study of risks faced by business entities in various sectors of the economy, as well as the search for effective methods of their neutralization. Among the scientists who devoted their works to this topic, it is worth pointing out the following researchers: Bezverkhy K.V., Gordopolov V.Y., Nazarova K.O., Parasiy-Vergunenko I.M. systematically substantiated the theoretical and methodological foundations of risk management and quantitatively evaluated them [7; 8; 12]. Ostapets A.O.. focused on risk classification in IT -companies. V. Dergacheva and D. Matyash analyzed the specifics of risks of foreign economic activity and proposed ways to minimize them [4]. Koretska O, Khoteeva N. investigated aspects of risk formation of companies [5]. Ocheretiana O. V. presented the risk management methodology for the woodworking industry, while Tarasova K. I. focused on various scientific approaches to the classification of economic risks. Sytnyk V., Sytnyk N., Tomashkov S., Ogerchuk Y. formulated the conceptual

principles of risk management [9; 10]. At the same time, a number of tasks related to the analysis and audit of risks in the field of IT companies remain open. The influence of external and internal factors that form risks in IT -companies , which requires further scientific study and practical development.

The goal articles there is research on key aspects of the analysis and audit of IT companies' risks, determination of the impact of these risks on the activities of economic entities, as well as the development of a system of administrative measures for effective control and reduction of risks to an acceptable level.

Materials and methods. The research materials used: (a) the legal framework governing the activities of economic entities, in particular IT companies, as well as statistical data on their functioning; (b) scientific works by both Ukrainian and foreign authors investigating the issue of risk formation, in particular those specific to the field of IT companies. During the research, the following scientific methods were applied: theoretical generalization and classification, methods of formalization, analysis and synthesis, as well as logical generalization of the obtained results with the formulation of conclusions.

Presentation of the main material. The activities of IT companies in the field of entrepreneurship are constantly accompanied by risks. These risks can be caused by both external and internal factors, affecting the functioning of the business with different intensity. The conducted scientific research emphasizes that during the risk audit, it is necessary to clearly understand the sources of their occurrence and have a well-planned control strategy. This allows you to minimize the negative impact of risks on the activities of the IT company. Table 1 presents a brief description of the risk audit of IT companies depending on their types.

Table 1

Characteristics of the risk audit for enterprises IT - spheres

Name	Brief description
Audit of operational risks	Risks in an IT company arise due to internal problems in its processes, which may be caused by employee errors, technical malfunctions or failures of information systems. Situations such as incorrect data entry or computer equipment failure are capable of disrupting operational processes, which can cause delays in the functioning of the company.

	The audit of operational risks is aimed at a thorough study of the company's activities, its compliance with standards and regulatory documentation, as well as a detailed analysis of the factors that affect the formation of these risks.
Audit of financial risks	IT companies often face various financial risks, including insufficient financial resources, exchange rate fluctuations, changes in interest rates and risks associated with counterparty insolvency. In particular, the instability of exchange rates can cause additional costs for companies operating in international markets. Financial risk audits include analysis and verification of aspects such as financial statements, tax documentation, discipline in calculations and the general financial condition of the company .
Audit of legal risks	This type of risks is associated with changes in legislation or violation of current regulations, which can have a significant impact on the functioning of IT companies. The introduction of new tax regulations or modification of regulatory requirements may lead to an increase in costs or the creation of additional obligations to state bodies. For example, an increase in tax rates can increase the financial costs of a company, which in turn reduces its profitability. Failure to comply with established legal requirements may result in the imposition of fines, the application of legal sanctions or other restrictive measures that may negatively affect both the financial condition of the company and its business reputation. Conducting an audit of legal risks involves a comprehensive analysis of factors that may contribute to the deviation of the company's activities from the norms of legal regulation.
Audit of reputational risks	With the development of modern technologies and digitalization processes, IT companies are becoming more and more vulnerable to cyber threats. These threats can target financial systems, client databases, intellectual property, and other critical resources. The main range of risks includes theft or destruction of information, paralysis of systems, which can cause significant financial losses and disruptions in the company's activities. In addition, the publicity of such incidents can negatively affect the reputation of the IT company, which threatens to lose the trust of customers and partners. Audit of reputational risks consists in identifying and analyzing factors that affect the business reputation of the organization, among which we can single out the level of data security, the presence of internal cyber incidents, staff turnover and other aspects.

Source: formed by the authors based on the data [4; 6; 7; 8]

Theoretical studies have confirmed that one of the main problems in the modern management of IT companies is the underestimation of the importance of risk analysis and audit. As a custom, companies' attention is focused on solving short-term financial obligations, while strategic planning and the long-term consequences of debt dependence are often left out of focus. In such a context, risk analysis and audit play an important role not only as instruments for the verification of financial documents, but also as mechanisms for identifying and

reducing risks. The use of audit analysis and audit makes it possible to comprehensively assess the company's financial situation, identify critical threats in advance, predict the degree of dependence of the company's profitability indicators on them, as well as develop effective debt management strategies. The use of audit risk control gives IT-companies not only a monitoring tool, but also a means of preventing critical financial losses.

Allianz Risk Barometer [3] research finds that the biggest threats to IT business development, where risk analysis and audit are important, include the following factors: interruption of production processes; - pandemics and their consequences; cyber attacks and other incidents in the field of cyber security; market instability and growing competition; changes in legislation and regulatory regulation; natural disasters and natural disasters; explosions and fires; macroeconomic risks; climate change; political instability and related risks. A questionnaire study showed that 41% of respondents consider interruptions in production to be the main risk for the IT business. The list is followed by pandemic (40%) and cyber incidents (40%). Invariably, the risk of disruption of business processes remains the leading one. In particular, 59% of respondents cite the pandemic as the main cause of this risk, followed by cybercrimes, natural disasters, explosions and fires. It is worth noting that in the last decade, according to reports from the Allianz Risk Barometer, the pandemic has never risen above the 16th place among threats. However, the coronavirus pandemic clearly demonstrated weaknesses in the world economy and the unpreparedness of IT businesses for unpredictable shocks. Although cyber incidents have moved to the third position, they remain a significant threat to business development. Large-scale digitalization of processes and the transition to teleworking during the pandemic only increased the vulnerability of Internet technologies. For example, in the midst of the first wave of lockdowns in April 2020, the number of cyber incidents increased by 300%. At the same time, the economic damage from cybercrime reached 1 trillion dollars, which is 50% more than two years ago.

Changes in legislation and regulatory policy have lost ground over time, moving to fifth place (compared to the third five years ago). According to experts' forecasts, the adoption of new norms in the field of data protection and improvement of cyber resistance is likely in the coming years. Natural disasters have fallen from the fourth position of ten years ago to sixth place, but remain an important risk factor due to their devastating effects and significant material losses [13; 16]. This is particularly relevant for Asian regions that regularly face the impact of climate events. Although climate change ranks ninth in the ranking, global warming remains a key threat to the planet. Macroeconomic developments rose from 10th to 8th place due to changes in monetary policy, rising commodity prices, and deflationary and inflationary processes. Political risks are ranked last – mass riots are increasingly displacing the terrorist threat, affecting global political and economic stability. It is extremely important for the auditor during the evaluation and analysis of IT–risks to determine effective methods of their control. According to the authors, control methods should be classified into three main groups: risk reduction by rejecting or reducing it; hedging, which involves the transfer of risk; as well as risk acceptance with the simultaneous implementation of measures to reduce it. Risk reduction due to its deviation or reduction is characterized by the absence of activities or business operations that are potentially associated with threats, in order to completely eliminate the probability of risk occurrence and prevent its consequences. According to the international standard ISO 31000:2018, risk avoidance is considered as a conscious choice not to participate or to stop certain activities in order to avoid exposure to a specific risk [1; 2]. Hedging, or risk transfer, consists of delegating part of the risk management responsibilities to partners. The international standard ISO 31000:2018 defines risk transfer as the process of transferring or allocating risk to another party [1; 2]. This standard also provides for conscious risk-taking, which includes holding the likelihood of risk occurring without additional measures to reduce, avoid or transfer it. As part of the analysis of the

impact of personnel potential, in particular technical IT specialists in leading companies in the IT sphere, and the formation of operational risks, a study was conducted using data on the staffing of IT companies, which are summarized in Table 2.

This study aims to address the key challenges related to risk assessment and audit in IT business. 10 leading IT companies were chosen for analysis by mechanical method.

Table 2

Analysis of the coefficients of provision by leading technical specialists IT-companies of Ukraine for the period 2021 – 2025

Name of the company entity	2021 (Pre-war period)			2024 (War period)			2025 (War period)			Deviation, coef. (+,–)	
	In total, there was work by specialists in the IT sphere, ps.	of which:		In total, there was work by specialists in the IT sphere, ps.	of which:		In total, there was work by specialists in the IT sphere, ps.	of which:		2025 for 2021	2025 for 2024
		Technical specialists-allists, ps	Coefficient of provision of technical specialists, ps.		Technical specialists-allists, ps	Coefficient of provision of technical specialists, ps.		Technical specialists-allists, ps	Coefficient of provision of technical specialists, ps.		
EPAM Ukraine	11600	10700	0,92	9350	8630	0,92	9350	8630	0,92	–	–
SoftServe	9462	7482	0,79	7242	5618	0,78	7242	5608	0,77	-0,02	–
GlobalLogic Ukraine	6365	5901	0,93	5466	5134	0,94	5465	5134	0,94	0,01	–
Ajax Systems	1800	320	0,18	3913	1167	0,30	3913	1167	0,30	0,12	–
Genesis	1683	1027	0,61	3156	1317	0,42	3156	1317	0,42	-0,19	–
Evoplay	2345	1415	0,60	2476	1740	0,70	2476	1740	0,70	0,10	–
DataArt	2625	2320	0,88	2139	1836	0,86	2139	1836	0,86	-0,03	–
Ciklum	3006	2513	0,84	1950	1783	0,91	1950	1783	0,91	0,08	–
Sigma Software	1500	1280	0,85	1832	1385	0,76	1832	1385	0,76	-0,10	–
ZONE3000	2004	1614	0,81	2290	1902	0,83	2252	1866	0,83	0,02	–

Source: calculated by authors on the basis of [17]

The results of the study show that in the pre-war period in Ukraine (until 2022), the coefficient of provision of technical specialists in IT companies demonstrated a change in dynamics compared to forecasts for 2024–2025. The analysis also indicates that during martial law there was relative stability in the formation of personnel due to the fact that some companies experienced a reduction in the number of specialists, while in others their number increased. In particular, in 2025, compared to 2021, a decrease in the ratio of provision of technical specialists was recorded in the companies SoftServe, Genesis, DataArt and Sigma Software. At the same time, this indicator grew in such companies as GlobalLogic Ukraine, Ajax Systems, Evoplay, Ciklum and ZONE3000. The situation shows that the structure of personnel potential significantly affects the activities of IT companies. Insufficient numbers of technicians create risks of financial loss, raising the overall level of entrepreneurial risk of an entire sector. Unskilled personnel, weak motivation, internal conflicts or bad faith of employees, in particular cases of fraud, can cause significant reputational losses, financial losses and deterioration of profitability indicators.

Reducing these risks is possible only thanks to a careful approach to personnel selection, constant training, organization of team events (team building) and reasonable distribution of responsibilities among employees of IT companies. Research experts consider it necessary to identify several key types of personnel risks characteristic of the IT sphere:

– risk of worker overload: arises from misallocation of responsibilities, which provokes stressful states, reduced productivity and the possibility of conflicts;

– risk of employee bad faith: errors at the hiring stage (for example, insufficient screening of candidates) can lead to theft, abuse and financial loss;

– risk of underqualification: when the level of knowledge or skills of employees does not meet the requirements of their positions, it negatively affects the efficiency of the company and increases the probability of making mistakes;

– reputational risks: unethical behavior of employees, internal conflicts or a low level of corporate culture can harm the image of the company.

The results of the conducted research make it possible to single out the key tasks of risk analysis in the field of activity of IT companies. Such tasks include:

– formation of a comprehensive list of threats, including external and internal factors that may affect the functioning of the company, its assets, reputation, as well as personnel;

– assessment of the probability of risk situations and measurement of the amount of potential losses, which can be both financial and time;

– analysis of the root causes of risks, which allows a deeper understanding of the sources of threats; - assessment of the company's ability to resist negative impacts and effectively recover after their implementation;

– development of a strategic action plan aimed at minimizing the consequences of threats through their prevention, insurance, transfer or risk acceptance;

– systematic review of the company's risk profile to update assessments and adapt risk management measures to changing conditions.

Performing risk analysis tasks will contribute to IT companies not only in adapting to challenges, but also in making informed management decisions that will ensure their stability and increase profitability. The main purpose of risk audits is to identify, assess and analyze potential threats, such as financial, operational or reputational risks, which may stand in the way of achieving the company's strategic goals. In addition, the audit includes the development of recommendations for effective risk management or their bias. In the process, a detailed analysis of internal control systems is carried out and the reliability of business processes is assessed to ensure their compliance with the company's requirements and needs.

The main tasks of risk audit in IT companies, in our opinion, include:

– identification of factors that pose a threat to the company's economic and financial activities (internal, external, operational, etc.);

– assessment of the degree of impact of each risk on financial reporting and the overall functioning of the enterprise;

– analysis of the effectiveness of measures implemented to prevent errors, fraud or financial losses;

– providing recommendations for optimizing business processes with the aim reducing risks and improving profitability;

– checking the ability of audit procedures to detect material misstatements in a timely manner.

Thus, risk audit is an important tool for making informed management decisions, ensuring the reliability of information, reliability and stability of the IT company's activities.

Conclusions and prospects for further research. Analysis and audit of risks carried out in IT companies involve a comprehensive and impartial assessment of information systems, technical infrastructure and business processes. This is done to identify possible vulnerabilities, ensure a high level of cyber security and comply with international standards such as ISO 27001 and GDPR. A comprehensive approach includes testing all elements of the technology environment, from hardware and software, access control systems and data backup policies, to developing business continuity plans. The main outcome of such analysis is the preparation of a report with detailed recommendations for risk mitigation and elimination. The conducted research made it possible to structure key aspects that form directions for effective analysis and audit:

– conducting a comprehensive analysis and audit of cyber security and data protection: identification of possible vulnerabilities, assessment of threats and risks, analysis of event logs, as well as verification of the reliability of personal and financial information protection systems;

– analysis and audit of the IT infrastructure to determine its stability and reliability: assessment of the state of hardware, software and networks, detection of potential failures, review of the effectiveness of backup systems;

– conducting a compliance audit (Compliance Audit): checking compliance of domestic policies with the requirements of international standards and regulations, such as GDPR or ISO 27001;

– execution of process audit: analysis of management procedures, monitoring of events and effectiveness of IT controls.

As a result, the authors highlight the main stages of the analysis and audit process: planning, inventory and analysis; identification and assessment of risks for IT companies; preparation of reporting based on the results of analysis and audit in order to create an effective control system.

In future scientific research, it is planned to focus on a detailed quantitative analysis of risks arising in IT companies, as well as on the study of the relationship between the level of risk and the financial indicators of their activity. The use of regression-correlation analysis is a promising tool that will contribute not only to the identification of the optimal level of acceptable risk, but also to the justification of measures for its systematic monitoring and control at the management level of the company. The implementation of this approach will enable the heads of IT companies to more effectively manage risks, promptly respond to emerging problems and threats, which will contribute to increasing the overall productivity of the organization and achieving optimal results of its work.

Література

1. ISO 31000:2018 Risk management – Guidelines. URL: https://www.iso.org/standard/65694.html (accessed: 01.12.2025).

2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/standard/27001 (accessed: 01.12.2025).

3. Allianz Risk Barometer: Identifying the major business risks. URL: https://surl.lu/oaosur (accessed: 01.12.2025).

4. Дергачова В. В., Матіяш Д. О. Управління ризиками зовнішньоекономічної діяльності підприємства [Risk management of foreign economic activity of the enterprise]. *Бізнес, інновації, менеджмент: проблеми та перспективи:* матеріали V Міжнародної науково-практичної конференції (Київ, 25 квітня 2024 р.). 2024. с. 134.

5. Корецька О. В., Хотєєва Н. В., Чиж Л. П. Міжнародні стандарти та статистичні методи щодо оцінки ризиків у діяльності міжнародних організацій [International standards and statistical methods regarding risk assessment in the activities of international organizations]. *Економіка та суспільство.* 2023. Вип. 52. URL: https://surl.lt/cdfqdc (accessed: 12.11.2025).

6. Кривда О., Очеретяна О. Аналіз та методика управління ризиками на підприємствах деревообробної промисловості. *Східна Європа: економіка, бізнес та управління.* 2020. Вип. 2 (25). С. 235–240. DOI: https://doi.org/10.32782/easterneurope.25-34

7. Nazarova K., Bezverkhyi K., Hordopolov V., Melnyk T., Poddubna N. Risk analysis of companies' activities on the basis of non-financial and financial statements. *Agricultural and Resource Economics.* 2021. Vol. 7, № 4. P. 180-199. URL: https://are-journal.com/are/article/view/484 (accessed: 01.12.2025).

8. Nazarova K., Nezhyva M., Moyseyenko O., Mysiuk V., Levkov K., Kucher A. Tourism risk audit under the COVID-19 impact. *Financial and credit activity: problems of theory and practice.* Kyiv, 2022. № 2(43). P. 53-62. DOI: https://doi.org/10.55643/fcaptp.2.43.2022.3608

9. Ситник В. Ф., Ситник Н. В. Дерева рішень в системах дейтамайнінгу. *Формування ринкової економіки.* 2006. Вип. 16. С. 442–454.

10. Томашков С. Б., Огерчук Ю. В. Оцінювання впливу ризиків зовнішньоекономічної діяльності. *Менеджмент та підприємництво в*

Україні: етапи становлення і проблеми розвитку. 2023. Вип. 2 (9). С. 142–151.

11. Балдинюк В. Ризик-менеджмент як інструмент управління діяльності суб'єктів господарювання. *Економіка та суспільство*. 2023. (55). DOI: https://doi.org/10.32782/2524-0072/2023-55-39

12. Безверхий К., Парасій-Вергуненко І., Гордополов В. Ризики в межах е-аудиту та напрямки їх мінімізації. *Збірник наукових праць Державного податкового університету.* 2025. № 1. С. 3–10. DOI: https://doi.org/10.32782/2617-5940.1.2025.1

13. Грицай О.І. Дефір І.В., Козак О.Є. Огляд кількісних методів оцінки ризиків зовнішньоекономічної діяльності. *Економіка і суспілство.* 2024. № 68. URL: https://surl.lt/ttxhra (accessed: 12.11.2025).

14. Кривда О., Кузьмінська Н., Драбенко Т. Аналіз кадрових ризиків аудиторських компаній. *Економіка та суспільство*. 2024. (61). DOI: https://doi.org/10.32782/2524-0072/2024-61-115

15. Овсієнко Н.В., Котвицька Н.М., Овсієнко В.В. Методичні підходи до створення стратегії управління ризиками сучасних підприємств. *Економічний простір.* 2025. № 197. URL: https://surl.li/resaek (accessed: 12.11.2025).

16. Остапець А. О., Парасій-Вергуненко І. М. (2025). Методики якісного аналізу ризиків підприємств галузі ІТ. *Міжнародний науковий журнал "Інтернаука". Серія: "Економічні науки".* 2025. № 2. DOI: https://doi.org/10.25313/2520-2294-2025-2-10724

17. ТОП-50 найбільших ІТ-компаній України. URL: https://surl.li/kvfrlr (accessed: 01.12.2025).

References

1. International Organization for Standardization. (2018). *ISO 31000:2018 Risk management – Guidelines*. https://www.iso.org/standard/65694.html

2. International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. https://www.iso.org/standard/27001

3. Allianz. (n.d.). *Allianz risk barometer: Identifying the major business risks*. https://surl.lu/oaosur

4. Derhachova, V. V., & Matiiash, D. O. (2024). Upravlinnia ryzykamy zovnishnoekonomichnoi diialnosti pidpryiemstva [Risk management of foreign economic activity of the enterprise]. In *Biznes, innovatsii, menedzhment: problemy ta perspektyvy: Materialy V Mizhnarodnoi naukovo-praktychnoi konferentsii* (Kyiv, April 25, 2024, p. 134) [in Ukrainian].

5. Koretska, O. V., Khotieieva, N. V., & Chyzh, L. P. (2023). Mizhnarodni standarty ta statystychni metody shchodo otsinky ryzykiv u diialnosti mizhnarodnykh orhanizatsii [International standards and statistical methods regarding risk assessment in the activities of international organizations]. *Ekonomika ta suspilstvo – Economy and Society*, 52. https://surl.lt/cdfqdc [in Ukrainian].

6. Kryvda, O., & Ocheretiana, O. (2020). Analiz ta metodyka upravlinnia ryzykamy na pidpryiemstvakh derevoobrobnoi promyslovosti [Analysis and methodology of risk management at woodworking industry enterprises]. *Skhidna Yevropa: ekonomika, biznes ta upravlinnia*, 2(25), 235–240. https://doi.org/10.32782/easterneurope.25-34 [in Ukrainian].

7. Nazarova, K., Bezverkhyi, K., Hordopolov, V., Melnyk, T., & Poddubna, N. (2021). Risk analysis of companies activities on the basis of non-financial and financial statements. *Agricultural and Resource Economics:*

International Scientific E-Journal, 7(4), 180–199. https://are-journal.com/are/article/view/484

8. Nazarova, K., Nezhyva, M., Moyseyenko, O., Mysiuk, V., Levkov, K., & Kucher, A. (2022). Tourism risk audit under the COVID-19 impact. *Financial and Credit Activity: Problems of Theory and Practice*, 2(43), 53–62. https://doi.org/10.55643/fcaptp.2.43.2022.3608

9. Sytnyk, V. F., & Sytnyk, N. V. (2006). Dereva rishen v systemakh deitamaininhu [Decision trees in data mining systems]. *Formuvannia rynkovoi ekonomiky*, 16, 442–454 [in Ukrainian].

10. Tomashkov, S. B., & Oherchuk, Yu. V. (2023). Otsiniuvannia vplyvu ryzykiv zovnishnoekonomichnoi diialnosti [Assessment of the impact of the risks of foreign economic activities]. *Menedzhment ta pidpryiemnytstvo v Ukraini: etapy stanovlennia i problemy rozvytku – Management and Entrepreneurship in Ukraine: The Stages of Formation and Problems of Development*, 2(9), 142–151 [in Ukrainian].

11. Baldyniuk, V. (2023). Ryzyk-menedzhment yak instrument upravlinnia diialnosti sub'iektiv hospodariuvannia [Risk management as a tool for managing the activities of business entities]. *Ekonomika ta suspilstvo*, (55). https://doi.org/10.32782/2524-0072/2023-55-39 [in Ukrainian].

12. Bezverkhyi, K., Parasii-Verhunenko, I., & Hordopolov, V. (2025). Ryzyky v mezhakh e-audytu ta napriamky yikh minimizatsii [Risks within e-audit and ways to minimize them]. *Zbirnyk naukovykh prats Derzhavnoho podatkovoho universytetu*, (1), 3–10. https://doi.org/10.32782/2617-5940.1.2025.1 [in Ukrainian].

13. Hrytsai, O. I., Defir, I. V., & Kozak, O. I. (2024). Ohliad kilkisnykh metodiv otsinky ryzykiv zovnishnoekonomichnoi diialnosti [Overview of quantitative methods of foreign economic activity risk assessment]. *Ekonomika i suspilstvo*, (68). https://surl.lt/ttxhra [in Ukrainian].

14. Kryvda, O., Kuzminska, N., & Drabenko, T. (2024). Analiz kadrovykh ryzykiv audytorskykh kompanii [Analysis of human resources risks of audit firms]. *Ekonomika ta suspilstvo*, (61). https://doi.org/10.32782/2524-0072/2024-61-115 [in Ukrainian].

15. Ovsiienko, N. V., Kotvytska, N. M., & Ovsiienko, V. V. (2025). Metodychni pidkhody do stvorennia stratehii upravlinnia ryzykamy suchasnykh pidpryiemstv [Methodological approaches to creating risk management strategies for modern enterprises]. *Ekonomichnyi prostir*, (197). https://surl.li/resaek [in Ukrainian].

16. Ostapets, A. O., & Parasii-Verhunenko, I. M. (2025). Metodyky yakisnoho analizu ryzykiv pidpryiemstv haluzi IT [Methods of qualitative risk analysis for it industry enterprises]. *Mizhnarodnyi naukovyi zhurnal "Internauka". Seriia: Ekonomichni nauky*, (2). https://doi.org/10.25313/2520-2294-2025-2-10724 [in Ukrainian].

17. TOP-50 naibilshykh IT-kompanii Ukrainy. (n.d.). https://surl.li/kvfrlr [in Ukrainian].