UDC 338.2:658.5
JEL: D81; M11

FEATURES OF RISK MANAGEMENT AND ORGANIZATION OF INTERNAL AUDIT AT INDUSTRIAL ENTERPRISES

©2020 GAVRYS P. O., GAVRYS M. O., GAVRYS O. M.

UDC 338.2:658.5
JEL: D81; M11

Gavrys P. O., Gavrys M. O., Gavrys O. M. Features of Risk Management and Organization of Internal Audit at Industrial Enterprises

This article is aimed at studying the problem of risk management at industrial corporations. It examines the nature of risk and its impact on the way the modern corporations operate. The main types of risks are analyzed on the example of their classification, developed and applied by the leading German insurance company Allianz. It among them are 10 main types of risks, including risks associated with IT systems in enterprises (in particular, cyber-crimes, failures of IT systems, leakage and loss of data), production and supply chain risks, risks of changes in legislation and regulatory policy (in particular, duties, trade wars, sanctions, protectionism), force majeure and natural disasters, changes in markets (increased competition, new competitors, fluctuations, stagnation and fall of markets), fires and explosions, climate changes, reputational risks, risks of new technologies and macroeconomic factors such as monetary policy, government austerity programs, inflation, changes in resource prices, etc. The examples of occurrence of such risks in real enterprises are given. The role and the importance of risk management at industrial corporations is determined. The model of three "lines of defense" in risk management of industrial enterprises is described, where the "first line" includes operational management and internal control mechanisms, the "second line" – the services of enterprises, responsible for management and control of risks on the ground, in particular, financial control, security service, services of quality control, compliance with standards and others, and the "third line" is internal audit. The practical aspects of its application are defined. The role and function of internal audit in risk management of companies is determined. The differences in scope and goals of internal audit as compared to other corporate compliance and governance functions are highlighted.

Keywords: *risk, risk management, industrial corporation, three lines of defense, internal audit, internal control system.*
DOI: *https://doi.org/10.32983/2222-4459-2020-9-128-135*
Fig.: *1.* ***Bibl.:*** *23.*

Gavrys Petro O. *– PhD (Economics), Corporate Auditor of the Department of Corporate Audit, Heraeus Holding GmbH (12–14 Heraeusstrasse, Hanau, 63450, Germany)*
E-mail: *petro.gavrys@gmail.com*
ORCID: *http://orcid.org/0000-0003-1493-8721*

Gavrys Mykola O. *– Senior Lecturer of the Department of Economic Analysis and Accounting, National Technical University «Kharkiv Polytechnic Institute» (2 Kyrpychova Str., Kharkiv, 61002, Ukraine)*
E-mail: *ngavrys@gmail.com*
ORCID: *http://orcid.org/0000-0001-8316-1472*

Gavrys Oleksandr M. *– PhD (Economics), Professor, Professor of the Department of Commercial, Trade and Entrepreneurial Activity, National Technical University «Kharkiv Polytechnic Institute» (2 Kyrpychova Str., Kharkiv, 61002, Ukraine)*
E-mail: *agavrys@gmail.com*
ORCID: *http://orcid.org/0000-0001-7394-6276*

УДК 338.2:658.5
JEL: D81; M11

Гаврись П. О., Гаврись М. О., Гаврись О. М. Особливості управління ризиками та організації внутрішнього аудита на промислових підприємствах

Метою статті є вивчення проблем управління ризиками на промислових підприємствах. Досліджується природа ризиків і їхній вплив на функціонування сучасних підприємств. Проаналізовано основні види ризиків на прикладі їхньої класифікації, що розроблена та застосовується провідною німецькою страховою компанією Allianz. Вона передбачає 10 основних видів ризиків, серед яких: ризики, пов'язані з IT-системами на підприємствах (зокрема, кібер-злочини, відмова IT-систем, витік і втрата даних); виробничі ризики та ризики ланцюга поставок; ризики змін у законодавстві та регуляторній політиці (у тому числі, мита, торговельні війни, санкції, протекціонізм); форс-мажори та природні катастрофи; зміни на ринках (загострення конкуренції, нові конкуренти, коливання, стагнація та падіння ринків); пожежі та вибухи; кліматичні зміни; репутаційні ризики; ризики нових технологій; а також макроекономічні чинники, такі як: монетарна політика; державні програми економії; інфляція; зміни цін на ресурси тощо. Наведено приклади виникнення таких ризиків на реальних підприємствах. Визначено роль та місце управління ризиками на промислових підприємствах. Описано модель трьох «ліній оборони» в управлінні ризиками промислових підприємств, де «перша лінія» включає операційний менеджмент і механізми внутрішнього контролю; «друга лінія» – служби підприємств, що відповідають за управління та контроль ризиків на місцях, зокрема фінансовий контроль, служби безпеки, контролю якості, відповідності стандартам та інші; «третя лінія» – внутрішній аудит. Обґрунтовано її застосування; визначено роль і функції внутрішнього аудиту

в управлінні ризиками підприємства. Виділено відмінності в цілях і функціях внутрішнього аудиту порівняно з іншими елементами системи управління ризиками підприємства.
Ключові слова: *ризик, управління ризиками, промислове підприємство, три «лінії оборони», внутрішній аудит, внутрішня система контролю.*
Рис.: *1.* ***Бібл.:*** *23.*

Гаврись Петро Олександрович *– кандидат економічних наук, внутрішній аудитор відділу внутрішнього аудиту, Хереус Холдінг ГмбХ (Хереусштрассе, 12-14, Ханау, 63450, Німеччина)*
E-mail: *petro.gavrys@gmail.com*
ORCID: *http://orcid.org/0000-0003-1493-8721*

Гаврись Микола Олександрович *– старший викладач кафедри економічного аналізу та обліку, Національний технічний університет «Харківський політехнічний інститут» (вул. Кирпичова, 2, Харків, 61002, Україна)*
E-mail: *ngavrys@gmail.com*
ORCID: *http://orcid.org/0000-0001-8316-1472*

Гаврись Олександр Миколайович *– кандидат економічних наук, професор, професор кафедри комерційної, торговельної та підприємницької діяльності, Національний технічний університет «Харківський політехнічний інститут» (вул. Кирпичова, 2, Харків, 61002, Україна)*
E-mail: *agavrys@gmail.com*
ORCID: *http://orcid.org/0000-0001-7394-6276*

Entrepreneurial activity is by definition associated with uncertainty, that is, it is risky, meaning that there is a certain probability it might result into undesirable and negative outcomes. Thus, risks are an important factor in planning and organizing business activities of enterprises. At the same time, there is direct relationship between the complexity of the processes, the size of the enterprise and the overall level of risks that may adversely affect the results of economic activities. The higher these values are, the greater the potential losses from the occurrence of these risks will be. That is why effective risk management is an important task of management and a key factor in achieving long-term success for large industrial enterprises.

Analysis of recent research on the topic. The concept of "risk" and risk management mechanisms in practice have always been and still are the subject of interest for many scientists and practitioners. For example, R. Picus defines the concept of "risk" from the enterprise viewpoint as "the probability of occurrence of a certain event that may result in losses of the expected economic benefits or direct losses" [1, p. 13]. Obviously, enterprises are directly interested in minimizing potential negative consequences of their economic activities, which may interfere with the achievement of the goal of long-term profitability, and in some cases even threaten the existence of enterprises. Accordingly, risk management, which can be defined as "a system of organizational and financial measures, united by a common idea and aimed at eliminating, preventing accidental unforeseen events, and limiting, minimizing losses, related to them", has become an important function in the enterprise [1, p. 15].

We'd like to highlight the following studies among the latest publications dedicated to the study of risks and risks management. R. Grinevsky [2] analyzes the risk management system from the user's viewpoint and evaluates such a system of response to negative factors as the method of "three lines of defense", which we also consider in this article. V. L. Dykan and I. M. Posokhov [3] study the international standards of risk management; P. Yo. Atamas, O. P. Atamas and G. O. Kramarenko [4] analyze the role of accounting in risk management; V. V. Romanenko [5] examines the European experience of risk management in taxation, and V. P. Bratyuk, K. Yu. Baisa [6] studies the features of the risk management process from the insurance company viewpoint. We'd also like to note more fundamental studies of foreign scientists, such as the works by P. Hopkin [7], J. Lam [8] and A. J. McNeil, R. Frey, P. Embrechts [9].

Thus, domestic and foreign scientists pay considerable attention to the problems of risk management; however, the issues of universal risk classification, which would be suitable for use by industrial enterprises, remain largely unresolved, and the role of internal audit, which is poorly developed in Ukraine, in the processes of risk management, remains virtually undisclosed.

In view of the above, the *purpose* of the article is to study the problems of risk management at industrial enterprises, in particular, the nature of risks and their impact on the functioning of enterprises;

major risks analysis on the example of their classification made by Allianz, the leading German insurance company; disclosure of the three "lines of defense" model and defining the role and functions of internal audit in the risk management at enterprises.

The main results of the study. In some form, risk management exists in almost every company, even if it is not a separate, clearly defined and consciously executed function. At the same time, building an effective risk management system is a difficult task, because the very concept of "risk" is quite abstract, and risks are very diverse in nature as well as difficult to generalize. For example, the leading German insurance company, Allianz, identifies the following ten main risk groups [10, p. 4–5]:

1. Risks associated with IT systems at enterprises.
2. Manufacturing risks and supply chain risks.
3. Risks of changes in legislation and regulatory policy.
4. Force majeure and natural disasters.
5. Changes in markets.
6. Fires and explosions.
7. Climate changes.
8. Reputational risks.
9. New technologies.
10. Macroeconomic factors.

The risks associated with IT systems at enterprises are manifold. The typical ones would include cybercrimes, failures of IT systems, leakage and loss of data, etc. An example of practical consequences of such risks has been a major data breach at one of the leading global hotel chains, Marriott International, revealed in late 2018, when the company announced that one of its reservation systems had been compromised, with hundreds of millions of customer records, including credit card and passport numbers, being stolen by the attackers [19]. In this case, data breach led to reputational losses, potential lawsuits and, presumably, lost revenues due to some customers' distrust of the company's ability to protect their personal data.

Manufacturing and supply chain risks are equally manifold and involve, for instance, risks of a key supplier not being able or willing to deliver materials of required quality on time and at acceptable prices. Such situation would lead to disruption of the company's production processes and inability to meet its own obligations to customers.

Risks of changes in legislation and regulatory policy might include tariffs, trade wars, sanctions, protectionism, etc. All of these might have major impact on operations, business model and might even jeopardize the very existence of the companies that get caught into such conflicts. A current example of the practical implications of such risks is the ongoing US-China trade conflict that has led to the US and China imposing tariffs on hundreds-billion–dollars' worth of one another's goods. Uncertainties around the trade war have hurt businesses and overburdened the global economy [11]. As a result, one of the major Chinese producers of smartphones and network equipment, Huawei, has been effectively banned from the US market, suffering extensive losses. The new sanctions that restrict any foreign semiconductor company from selling chips developed or produced using US software or technology to Huawei, without first obtaining a license to do so, might prove lethal to the Chinese tech giant [20].

The most recent example of the risks for business resulting from a force majeure has been the ongoing COVID-19 pandemics. Public policy measures introduced to contain the spread of COVID-19 are resulting in significant operational disruption for many companies. Staff under quarantine, failing supply chain, orphaned or unavailable inventories, and sudden reductions in demand from customers are creating serious challenges for companies across a wide range of sectors. Companies have faced months of exceptionally poor trading conditions and significant additional financing requirements. For many, the difficulties deriving from the exceptional circumstances are immediately converting into challenges at different levels of the organization [15]. For many companies from sectors that have been hit particularly hard by the pandemic, such as tourism or air travel, or companies with weaker balance sheets, such as Hertz, the challenges presented by the COVID-19 pandemics may prove to be fatal.

Changes in markets such as competition intensification, new competitors, fluctuations, stagnation and falling of markets, etc. might have significant impact on the companies operating in these markets. In some cases, new technologies and long term changes in customer behavior or preferences would lead to gradual decline of entire industries. An example of such disruption is the rise of the internet and digital media that led to a change in readers' behavior. Readers started using computers for reading with the internet as a key source of information rather than traditional printed media. This led to decline of both printing industry and printed media.

Another example of change in markets would be the appearance of a new competitor with a disruptive technology in an existing market. One current instance of such market disruption is the ongoing rise of Tesla, Inc., whose technology to produce electric vehicles has disrupted the existing automotive industry. As of August 2020, it has become by far the most valuable automotive company in the world by market capitalization [21].

Fires and explosions is another, more traditional category of business risks. The oil spill at Deepwater Horizon that resulted from an explosion and a fire at this off-shore oil drilling platform owned by British Petroleum, has had an estimated total cost to the company of around $65 billion [12].

Climate changes, while more difficult to quantify, play an increasingly important role in everyday life and might, in the long run, have significant impact on business as well. An example of such impact could be decrease in yields faced byagricultural companies as a result of changing weather patterns.

While reputation is not a tangible asset like machines, equipment or cash, its value should not be underestimated in the modern world where much depends on trust and relationship between business partners. Breach of trust between the partners and the resulting damaged relationships with, say, key customers might jeopardize the very existence of the companies that have suffered reputational losses. Although reputational risks are hard to measure, they might be of paramount importance for a company's future. The classic example of catastrophic consequences of reputational loss is Arthur Andersen, once the world's leading accounting and consulting company that collapsed in the aftermath of Enron accounting scandal, which had destroyed its reputation [22].

As mentioned above in the section on changes in markets, impact of the new technologies on existing companies in the industry might be crucial. The example of Tesla, Inc. with its electric vehicles shows that the new battery technology has completely disrupted the automotive industry and might even pose an existential threat to the "legacy" automakers whose products are mostly based on internal-combustion engines.

Finally, macroeconomic factors such as monetary policy, government austerity programs, inflation, changes in resource price, etc. might have major impact on profits and operating models of the companies affected by these factors. As commodities such as metals or agricultural products, e.g. wheat and sunflower oil, account for much of Ukraine's exports, many Ukrainian companies are very sensitive to fluctuations in global commodity prices. Significant decreases in commodity prices in global markets would immediately cause reduced revenues and, thus, threaten the companies' business models. Another example of the impact of microeconomic factors is the marked change in the monetary policy by the European Central Bank (ECB) since 2008 towards a significantly more expansive monetary policy and the so-called "quantitative easing", which is in fact nothing more than currency "printing", that is currency decaluation. The consequences of this policy are manifold. The immediate impact on individual businesses might differ. On the one hand, for instance, there are losers such as traditional banks, whose business models have been eroded by low interest rates that result into lower margins on credits issued by the banks. On the other hand, "quantitative easing" leads to the asset price inflation, e.g. for real estate, thus, giving a boost to real estate companies such as Vonovia, whose assets and revenues from the rising rents have soared as a result of the monetary policy by ECB [14].

While these are the ten most important risk categories to be faced by companies in 2020 according to Allianz, this list is far from exhaustive. Any of these categories can be detailed and expanded, as well as new, more specific risks, such as credit risks could be added. Also, as the nature of these risks is often complex, they might be overlapping, with the same risk being attributable to multiple categories, e.g. production disruption due to an IT failure resulting from a catastrophic event would be an IT, manufacturing and natural disaster related risk at the same time. Also, one can offer an alternative approach to the classification of risks, in particular, the division of risks into industrial, commercial, financial, legal and so on.

Another important feature of risks is that in many cases they are difficult to quantify, as they often depend on external factors, the probability and consequences of which are almost impossible to assess accurately and reliably.

Such heterogeneity and the complex nature of individual types of risks make it impractical to define risk management as a separate managerial function. Accordingly, in practice, companies prefer a more practical approach to risk management. They distribute the risk management function across dif-

ferent departments responsible for the day-to-day operations that give rise to individual risk types. By doing so, they ensure that both responsibility for and control over addressing specific risks lie with the people directly exposed to the risks. Accordingly, unnecessary bureaucracy is avoided and people with first-hand knowledge of risks are in control.

Still, this approach has some deficiencies as it fails to take into account more complex, strategic risks that might lie outside the area of responsibility of an individual department, e.g. risks of changing markets, potentially new products, competitors etc. that might have major impact on a company's business model. Also, this approach largely ignores important risks that might be beyond the competence level of people responsible for day-to-day operations where these risks arise. As an example of such more complex risks, we can name a currently very widespread type of specific cybercrime related fraud risks that involve payment diversion. In this case, impostors posing as a company's vendor break into a communication between the company and the vendor and at some point try to overtake the communication and convince the company to make payments of currently unpaid vendor invoices to a bank account different from the vendor's bank account, claiming the vendor bank data has been changed. Usually, they already have some insider knowledge of the relations between the company and the vendor as well as the payment status of vendor invoices. Normally, they get this sensitive information either by hacking communication between the vendor and the company, e.g. via infected emails, or by bribing employees of the vendor or the company. Since impostors have insider knowledge of the relationship between the company and the vendor, it is relatively easy for them to trick unsuspecting payment clerks at the company into making payments to some fraudulent bank accounts. Therefore, concerted action of the company's management and all the departments involved is required. The response to this risk should involve the IT department, master data management department and accounts payable department and should result into process change for making payments to new bank accounts by requiring independent confirmations by vendors prior to changing bank data and making payments to new vendor bank accounts. As some risks are too complex to be effectively dealt with by the immediately involved departments (in this case: accounts payable department) only, a more strategic approach to risk management is needed. This is why the overall responsibility for the development and implementation of risk management strategy rests with the management of the enterprise. At the same time, separate departments of the enterprise are responsible for the direct development of structures, mechanisms and processes, that should help to achieve an acceptable level of individual risks, associated with the operational activities of these departments [13].

In theory, we can distinguish three of the so-called "lines of defense" in risk management at enterprises (*Fig. 1*) [17, p. 2; 4, p. 69].

The first "line of defense" is the operational level of management at an enterprise, which is responsible for evaluation, control and neutralization of risks and effective functioning of the internal control system [16, p. 9]. Examples of such mecha-

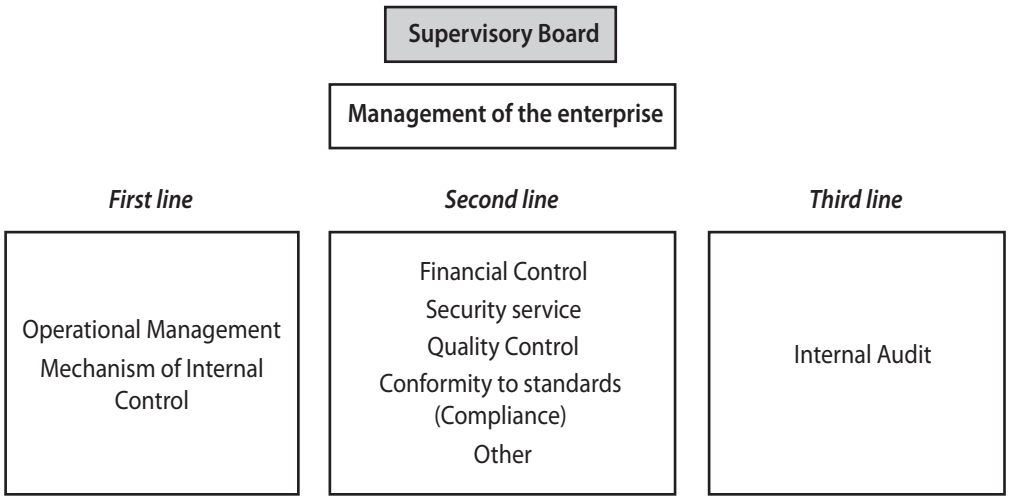

Fig. 1. The model of "three lines of defense" in risk management of the enterprise

nisms of the internal control system are the following: approval by customers of all invoices, received from suppliers, before payment, or the technical requirement for additional approval by an authorized person of all payments before debiting funds from the company's accounts [18].

The second "line of defense" includes special functions at an enterprise, which are responsible for compliance with standards in their specific areas. Such functions may include the following: financial control (compliance with financial discipline and prevention of financial frauds), security service (responsibility for the safekeeping of tangible and intangible assets), quality control (ensuring the compliance with a certain level of production quality), technical inspection (ensuring the satisfactory condition of technical equipment and devices) and compliance with standards (compliance with internal and external regulations).

Finally, the function of the last, third "line of defense" in risk management is performed by internal audit. Its main tasks are the following: to provide independent and objective conclusions on the effectiveness of risk management, mechanisms of corporate governance and internal control systems [23], including the effectiveness of the first and second "lines of defense", as well as recommendations concerning their improvement.

The functions of internal audit are significantly different compared to the functions of departments, designed to evaluate and manage the risks of an enterprise. Compared to operational management, the main difference is that internal audit is not responsible for the operational activities of an enterprise, building the internal control system and the risk management system. Internal audit provides an independent evaluation of the effectiveness of internal control and risk management systems, implemented at the operational level.

Similarly, significant differences between internal audit and the functions, responsible for compliance with standards in their specific areas, are that internal audit does not define or implement internal standards at an enterprise, but only controls whether these standards have been fully implemented in specific departments.

Another feature of internal audit is that it is not part of the standard organizational structure of an enterprise, but is a separate, independent department, that reports directly to the board of directors or the executive board of an enterprise, which allows it to maintain impartiality and objectivity.

If we compare the internal and external audit, the main differences lie, first of all, in the tasks and scope of activities, and not in the features of organizational affiliation. The main task of external audit is to confirm that the financial statements of an enterprise are created in accordance with certain standards and the facts, presented in these statements, are generally true. Accordingly, external audit is usually limited to the audit of financial statements and its separate components. It is not supposed to evaluate the internal control systems or the effectiveness of processes. At the same time, internal audit is focused on completely different tasks. Verification of financial statements and accounting records is its secondary task only, while among the priorities of internal audit are the following:

1. Checking the effectiveness of the internal control systems functioning;
2. Verification of compliance with internal and external standards and instructions;
3. Verification of ensuring the safekeep of material values at an enterprise;
4. Checking the effectiveness of the risk management system;
5. Checking the effectiveness of particular processes at an enterprise;
6. Providing recommendations to improve the internal control systems and specific processes.

So, we can consider the different functions of internal and external audit as the result of their different objectives. External audit should ensure the interests of the investors and creditors of an enterprise, so its main purpose is to confirm the information, presented in the financial statements. At the same time, internal audit is part of the company, so it should help to achieve its strategic goals, namely, ensuring the long-term viability and profitability of the company by creating an effective and functional risk management system, internal control system as a whole and control of specific processes.

CONCLUSIONS

In the course of economic activity, each enterprise faces numerous challenges. How the enterprise responds to these challenges is one of the key factors, determining its long-term success. Moreover, risk management, which aims to prevent the occurrence of accidental unforeseen events, that can lead to negative consequences, eliminate or at least minimize these consequences, is becoming an increasingly important task for management. At the

same time, general trends, such as globalization, the spread of information technologies and the complexity of production processes and supply systems, are creating an increasingly complex environment for businesses, and thus increasing the risks, associated with doing business in such an environment. In these circumstances, an important role in ensuring effective risk management at an enterprise is played by internal audit, which is designed to provide independent and objective evaluation of the effectiveness of internal control systems and specific processes at an enterprise and recommendations for their improvement. ■

LITERATURE

1. Пікус Р. В. Управління фінансовими ризиками : навч. посіб. Київ : Знання, 2010. 598 с.
2. Гріневський Р. Система управління ризиками: кому і коли це потрібно. URL: http://www.management.com.ua/qm/qm245.html
3. Дикань В. Л., Посохов І. М. Дослідження міжнародних стандартів управління ризиками. *Бізнес Інформ*. 2014. № 1. С. 314–319. URL: https://www.business-inform.net/export_pdf/business-inform-2014-1_0-pages-314_319.pdf
4. Атамас П. Й., Атамас О. П., Крамаренко Г. О. Роль бухгалтерського обліку в управлінні ризиками підприємництва. *Академічний огляд*. 2016. № 1. С. 60–69. URL: https://acadrev.duan.edu.ua/images/stories/files/2016-1/8.pdf
5. Романенко В. В. Європейський досвід управління ризиками в оподаткуванні. *Науковий вісник Національного університету державної податкової служби України (економіка, право)*. 2014. № 1. С. 253–258. URL: http://ndi-fp.nusta.com.ua/report/publication/20151112142923.pdf
6. Братюк В. П., Байса К. Ю. Особливості процесу управління ризиками, прийнятими на страхування. *Економічний аналіз*. 2014. Т. 17. № 1. С. 112–119. URL: https://www.econa.org.ua/index.php/econa/article/view/592/346
7. Hopkin P. Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. London : Kogan Page Publishers, 2010. 358 p.
8. Lam J. Enterprise Risk Management: From Incentives to Controls. 2nd ed. John Wiley & Sons, 2014. 496 p.
9. McNeil A. J., Frey R., Embrechts P. Quantitative Risk Management: Concepts, Techniques and Tools. Princeton University Press, 2015. 720 p.
10. Allianz Risk Barometer: Identifying the Major Business Risks For 2020. Allianz Global Corporate & Specialty SE, Munich, Germany, 2020. 23 p.
11. A quick guide to the US-China trade war // British Broadcasting Corporation. URL: https://www.bbc.com/news/business-45899310
12. Bousso R. BP Deepwater Horizon costs balloon to $65 billion // Thomson Reuters. URL: https://www.reuters.com/article/us-bp-deepwaterhorizon/bp-deepwater-horizon-costs-balloon-to-65-billion-idUSKBN1F50NL
13. Bungartz O. Handbuch Interne Kontrollsysteme (IKS): Steuerung und Überwachung von Unternehmen. Berlin, 2009. 480 p.
14. Call auf Vonovia: EZB deutet mehr billiges Geld an // onvista media GmbH. URL: https://www.onvista.de/news/call-auf-vonovia-ezb-deutet-mehr-billiges-geld-an-258512087
15. COVID-19 impact and business stabilization // Deloitte AG. URL: https://www2.deloitte.com/ch/en/pages/about-deloitte/articles/about-deloitte.html
16. Guidance on the 8th EU Company Law Directive, article 41 // European Confederation of Institutes of Internal Auditing (ECIIA)/ Federation of European Risk Management Associations (FERMA). Brussels, 2010. 19 p.
17. IAA Position Paper: The Three Lines of Defense in Effective Risk Management and Control / The Institute of Internal Auditors. Altamonte Springs, FL, USA, 2013. 7 p.
18. Internal Control – Integrated Framework / Committee of Sponsoring Organizations of the Treadway Commission (COSO). Durham, NC, USA, 2012. 194 p.
19. Marriott data breach FAQ: How did it happen and what was the impact? // CSO by IDG Communications Inc. URL: https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html
20. New sanctions deal 'lethal blow' to Huawei. China decries US bullying // Cable News Network. Turner Broadcasting System, Inc. URL: https://edition.cnn.com/2020/08/17/tech/huawei-us-sanctions-hnk-intl/index.html
21. Teslanomics: How to justify being the most valuable car company on earth // Fortune Magazine. URL: https://fortune.com/2020/08/10/tesla-most-valuable-car-company-in-the-world-electric-vehicles-evs/
22. The Fall of Andersen // Chicago Tribune. URL: https://www.chicagotribune.com/news/chi-0209010315sep01-story.html
23. What is Internal Audit / Chartered Institute of Internal Auditors. URL: https://www.iia.org.uk/about-us/what-is-internal-audit/

REFERENCES

"A quick guide to the US-China trade war". British Broadcasting Corporation. https://www.bbc.com/news/business-45899310

Allianz Risk Barometer: Identifying the Major Business Risks For 2020. Munich, Germany: Allianz Global Corporate & Specialty SE, 2020.

Atamas, P. I., Atamas, O. P., and Kramarenko, H. O. "Rol bukhhalterskoho obliku v upravlinni ryzykamy pidpryiemnytstva" [The Role of Accounting in Busi-

ness Risk Management]. Akademichnyi ohliad. 2016. https://acadrev.duan.edu.ua/images/stories/files/2016-1/8.pdf

Bousso, R. "BP Deepwater Horizon costs balloon to $65 billion". Thomson Reuters. https://www.reuters.com/article/us-bp-deepwaterhorizon/bp-deepwater-horizon-costs-balloon-to-65-billion-idUSKBN1F50NL

Bratiuk, V. P., and Baisa, K. Yu. "Osoblyvosti protsesu upravlinnia ryzykamy, pryiniatymy na strakhuvannia" [Features of Management Risks Process, Accepted on Insurance]. Ekonomichnyi analiz. 2014. https://www.econa.org.ua/index.php/econa/article/view/592/346

Bungartz, O. *Handbuch Interne Kontrollsysteme (IKS): Steuerung und Uberwachung von Unternehmen.* Berlin, 2009.

"Call auf Vonovia: EZB deutet mehr billiges Geld an". onvista media GmbH. https://www.onvista.de/news/call-auf-vonovia-ezb-deutet-mehr-billiges-geld-an-258512087

"COVID-19 impact and business stabilization". Deloitte AG. https://www2.deloitte.com/ch/en/pages/about-deloitte/articles/about-deloitte.html

Dykan, V. L., and Posokhov, I. M. "Doslidzhennia mizhnarodnykh standartiv upravlinnia ryzykamy" [Study of International Standards of Risk Management]. Biznes Inform. 2014. https://www.business-inform.net/export_pdf/business-inform-2014-1_0-pages-314_319.pdf

"Guidance on the 8th EU Company Law Directive, article 41". European Confederation of Institutes of Internal Auditing (ECIIA)/ Federation of European Risk Management Associations (FERMA). Brussels, 2010.

Hopkin, P. *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*. London: Kogan Page Publishers, 2010.

Hrinevskyi, R. "Systema upravlinnia ryzykamy: komu i koly tse potribno" [Risk Management System: Who Needs It and When]. http://www.management.com.ua/qm/qm245.html

IAA Position Paper: The Three Lines of Defense in Effective Risk Management and Control. Altamonte Springs, FL, USA: The Institute of Internal Auditors, 2013.

Internal Control – Integrated Framework. Durham, NC, USA: Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2012.

Lam, J. *Enterprise Risk Management: From Incentives to Controls.* John Wiley & Sons, 2014.

"Marriott data breach FAQ: How did it happen and what was the impact?". CSO by IDG Communications Inc. https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html

McNeil, A. J., Frey, R., and Embrechts, P. *Quantitative Risk Management: Concepts, Techniques and Tools*. Princeton University Press, 2015.

"New sanctions deal 'lethal blow' to Huawei. China decries US bullying". Cable News Network. Turner Broadcasting System, Inc. https://edition.cnn.com/2020/08/17/tech/huawei-us-sanctions-hnk-intl/index.html

Pikus, R. V. *Upravlinnia finansovymy ryzykamy* [Financial Risk Management]. Kyiv: Znannia, 2010.

Romanenko, V. V. "Yevropeiskyi dosvid upravlinnia ryzykamy v opodatkuvanni" [European Experience of Risk Management in Taxation]. Naukovyi visnyk Natsionalnoho universytetu derzhavnoi podatkovoi sluzhby Ukrainy (ekonomika, pravo). 2014. http://ndi-fp.nusta.com.ua/report/publication/20151112142923.pdf

"Teslanomics: How to justify being the most valuable car company on earth". Fortune Magazine. https://fortune.com/2020/08/10/tesla-most-valuable-car-company-in-the-world-electric-vehicles-evs/

"The Fall of Andersen". Chicago Tribune. https://www.chicagotribune.com/news/chi-0209010315sep01-story.html

"What is Internal Audit". Chartered Institute of Internal Auditors. https://www.iia.org.uk/about-us/what-is-internal-audit/