UDC 658.6:004.738.5 (339.13)

Natorina A.O.,
alyonanatorina@gmail.com, ORCID ID: 0000-0001-6367-879X,
Researcher ID: G-9089-2017,
Ph.D., Head of the International Economics, Accounting and Finance Department, Academician Yuriy Bugay International Scientific and Technical University, Kyiv

ESSENCES OF ONLINE BUSINESS MANAGEMENT: IT ASPECT

Abstract. *It is substantiated that the rational management of IT risks is the catalyst for the dynamic online business development in the context of digital transformation and changing marketing environment. It forms the foundation for the active relevant actions implementation to increase the online business competitiveness in accordance with its vision, mission and allows to achieve the planned metrics in the shortest possible time. The systematized list of IT risks of online business which divided into three groups (IT maintenance and support risks; IT potential management risks; IT administration risks) is developed and its graphical interpretation is given. The proposed IT risks take into account the specifics of digital transformation and its impact on the online business set and development. The scientific and methodical approach to assessing the probability of IT risks and making correct management decisions to level or eliminate them in the future is substantiated. The scientific and methodical approach involves the identification of the status of the IT risks online business, taking into account which allows to develop the relevant management plan. The proposed scientific and methodical approach is tested by the example of Ukrainian retailers that have online business in different market segments (food retail; drogerie; home appliances and electronics retail; DIY-retail). The preconditions and causes of online business IT risks of the studied set of Ukrainian retailers in clusters are determined. Reasonable explanations are given on the significance and likelihood of the online business IT risks of retailers in accordance with their identified statuses. It is developed the continuum of unified activities to reduce the negative consequences of three groups IT risks. It based on the results of testing the justified scientific and methodical approach.*

Key words: online business, retail, IT risk, qualitative assessment of IT risks, cybersecurity, cyberincident, continuum of unified activities.

Наторіна А. О.,
alyonanatorina@gmail.com, ORCID ID: 0000-0001-6367-879X,
Researcher ID: G-9089-2017,
к.е.н., завідувач кафедри міжнародної економіки, обліку та фінансів, Міжнародний науково-технічний університет імені академіка Юрія Бугая, м. Київ

ЕСЕНЦІЇ МЕНЕДЖМЕНТУ ОНЛАЙН-БІЗНЕСУ: ІТ-РАКУРС

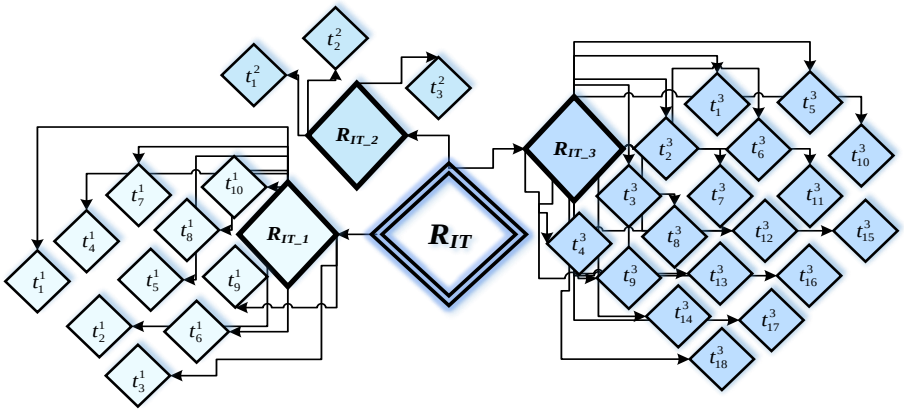
Анотація. *Обґрунтовано, що каталізатором динамічного розвитку онлайн-бізнесу в умовах цифрової трансформації та мінливому маркетинговому середовищі є раціональний менеджмент ІТ-ризиків. Він формує фундамент для реалізації активних релевантних дій з підвищення конкурентоспроможності онлайн-бізнесу відповідно до його візії, місії та дозволяє досягти заплановані метрики у максимально можливі короткі часові терміни. Розроблено систематизований перелік ІТ-ризиків онлайн-бізнесу у розрізі трьох груп (ризики ІТ-забезпечення та підтримки; ризики управління ІТ-потенціалом; ризики ІТ-адміністрування) та наведено його графічну інтерпретацію. Запропоновані ІТ-ризики враховують особливості цифрової трансформації та її вплив на ведення і розвиток онлайн-бізнесу. Обґрунтовано науково-методичний підхід щодо оцінювання ймовірності настання ІТ-ризиків та прийняття коректних управлінських рішень щодо їх нівелювання або ліквідації у перспективі. Науково-методичний підхід передбачає ідентифікацію статусів ІТ-ризиків онлайн-бізнесу, врахування яких дозволяє розробити релевантний план менеджменту. Апробовано запропонований науково-методичний підхід на прикладі українських ритейлерів, що здійснюють ведення онлайн-бізнесу у різних ринкових сегментах (food-ритейл; дрогери; ритейл у сфері побутової техніки та електроніки; DIY-ритейл). Детерміновано передумови та причини виникнення ІТ-ризиків онлайн-бізнесу досліджуваної сукупності українських ритейлерів у розрізі кластерів. Аргументовано надано роз'яснення щодо значущості та ймовірності настання ІТ-ризиків онлайн-бізнесу ритейлерів відповідно до їх ідентифікованих статусів. Розроблено континуум уніфікованих заходів зі зменшення негативних наслідків ІТ-ризиків у розрізі трьох груп, базуючись на результатах апробації обґрунтованого науково-методичного підходу.*

Ключові слова: онлайн-бізнес, ритейл, ІТ-ризик, кваліативне оцінювання ІТ-ризиків, кібербезпека, кіберінцидент, континуум уніфікованих заходів.

JEL Classification: G32, L81, M15.
DOI: https://doi.org/10.36477/2522-1205-2020-59-13

Statement of the problem. In the context of digital transformation, online business is constantly changing and involves the use of new approaches to IT implementation. It is also can be observed the constant increase in requirements for ensuring cybersecurity through the rapid development of malware, which, among other things, hinders the proper implementation of business processes. In these conditions, the dynamic development of online business requires systematic tracking of IT risks and the implementation of activities to level and / or eliminate cyberincidents and negative consequences if they occur.

Analysis of the latest research and publications. The impact of information and communication technologies on doing business in the national and international markets, as well as possible risks and consequences as a result of IT implementation are highlighted in the works [3; 7; 12]. The importance and role of risk management realization for the dynamic business development are shown in the publications [1-2; 10-11]. Nevertheless, the [4-6; 13-14] are determined the aspects of business management in various areas, taking into account certain types of risks. However, it is important to note that the specifics of online business management and development still require further research in the context of digital transformation and constant changes in the environment. In addition, a detailed interpretation of IT risks, which is necessary to take into account a successful online business, is still missing in scientific studies.



Notes.

R_{IT_1} – IT maintenance and support risks. Group 1: t_1^1 – insufficient management interest in IT implementation; t_2^1 – inadequate understanding of IT tasks and incorrect interpretation of IT problems; t_3^1 – untimely IT solutions; t_4^1 – irregular tracking of inquiries, needs and preferences of online buyers; t_5^1 – non-congruence of IT and business strategies; t_6^1 – inability to identify the IT needs of online business; t_7^1 – use of irrelevant IT tools; t_8^1 – lack or insufficiently clear budget allocation for IT development; t_9^1 – improper oversight of IT costs; t_{10}^1 – high level of dependence on the functioning of a number of information systems.

R_{IT_2} – IT potential management risks. Group 2: t_1^2 – unsatisfactory performance of the IT department's functions to ensure information and cybersecurity for successful online business in the market; t_2^2 – low qualification of IT department specialists; t_3^2 – statutory and regulatory inconsistencies of the IT department.

R_{IT_3} – IT administration risks. Group 3: t_1^3 – insufficient IT rationalization; t_2^3 – lack of control over the architecture of the information system; t_3^3 – inconsistency of IT standards; t_4^3 – unsatisfactory outsourcing control and / or excessive dependence on it; t_5^3 – incomplete monitoring of IT service levels; t_6^3 – lack of positive business results as a result of changes in IT administration; t_7^3 – incorrect operation of the continuous IT control system; t_8^3 – low level of determination and administration of cyberincidents; t_9^3 – irrational management of IT operations; t_{10}^3 – inability to manage the continuity of IT operations; t_{11}^3 – inconsistency of IT administration and business processes; t_{12}^3 – low quality IT testing; t_{13}^3 – complexity of the IT transformations administration and implementation; t_{14}^3 – generation of false data by the information system; t_{15}^3 – failure of data quality control; t_{16}^3 – weak protection of information system and IT equipment; t_{17}^3 – incorrect implementation of the cyberattack identification process; t_{18}^3 – disability of the cyberattack response system.

Fig. 1. IT risks of online business ***(developed by the author)***

Therefore, **the purposes** of the article are to systematize IT risks of online business and substantiate the scientific and methodical approach to assessing the likelihood of their occurrence, as well as develop the continuum of unified activities to reduce the negative consequences of these IT risks.

Results. The rational IT risk management in the context of digital transformation plays a key role in the development of online business in a changing marketing environment. It is the foundation for developing proactive actions to strengthen competitive market positions with mission, vision and desired metrics. Considering the above, according to the results of the detailed analysis of research by scientists [1-7; 10-14], the systematic list of online business IT risks is developed (Fig. 1) that, compared to others, takes into account the features and impact of digital transformation.

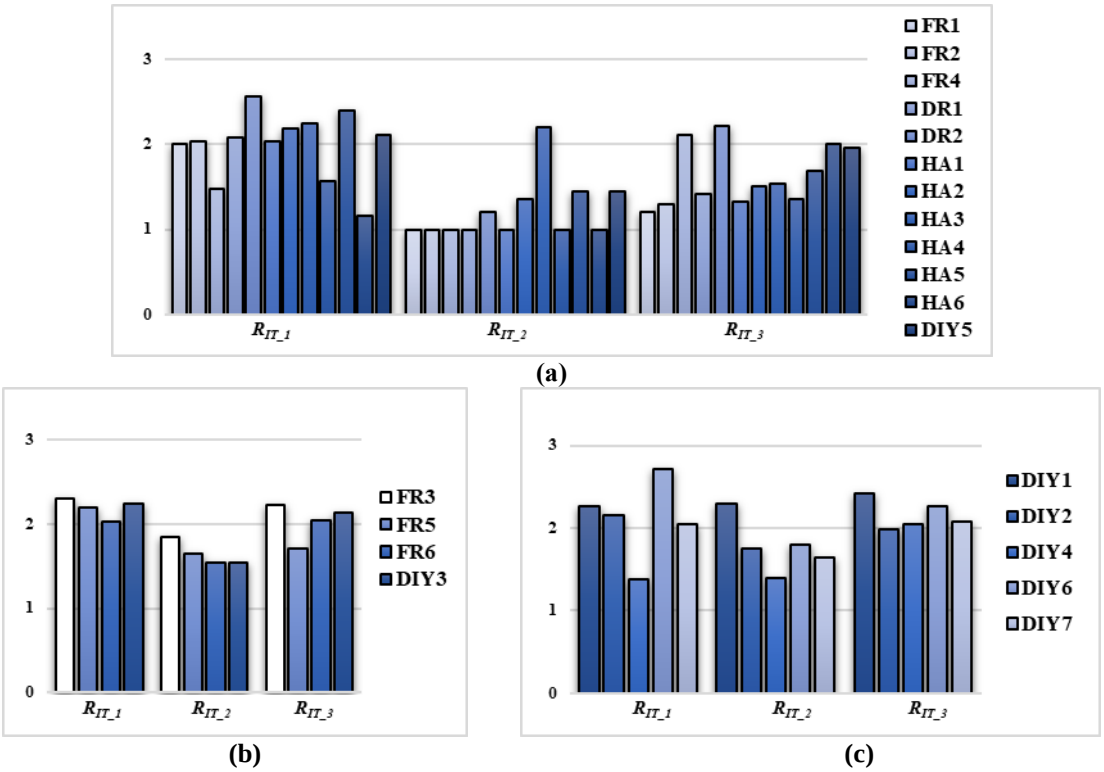
According to the Fig. 1, R_{IT} includes three risk groups (1):

$$R_{IT} = \{R_{IT\_1}; R_{IT\_2}; R_{IT\_3}\}, \quad (1)$$

where $R_{IT\_1} = \sum_{n=1}^{10} t_n^1$, $R_{IT\_2} = \sum_{n=1}^{3} t_n^2$, $R_{IT\_3} = \sum_{n=1}^{18} t_n^3$ (2-4)

The formation of the appropriate database of online business IT risks is the basis of the author's scientific and methodical approach to assess the probability of IT risks and make the right decisions to level or eliminate them in the future. The essence of the scientific and methodical approach is to survey experts and specialists in order to identify two statuses of IT risks – "accept" (status 1) and "change" (status 2, which divided into three types – "reduce", "transfer", "remove (eliminate)". The identified status allows to develop the relevant online business IT risk management plan.

The approbation of the scientific and methodical approach is carried out by the example of Ukrainian retailers who have online business in the following segments: food retail; drogerie; home appliances and electronics retail; DIY-retail. The division of retailers into clusters and certain aspects of their activities are reflected in [8-9]. The Fig. 2 represents the results of three groups of R_{IT} risks assessment of retailers' online business in 2020 in terms of three clusters.



(a) **(b)** **(c)**

Notes. *Cluster 1:* Auchan Ukraine (FR1), Metro Cash and Carry Ukraine (FR2), NOVUS Ukraine (FR4), Yves Rocher Ukraine (DR1), RUSH (DR2), ALLO (HA1), Foxtrot (HA2), DIESA (HA3), Comfy Trade (HA4), Harazh Mobail Hrup (HA5), Citrus Discount (HA6), Leroy Merlin Ukraine (DIY5). *Cluster 2:* NASH KRAI (FR3), Tavria V (FR5), Fozzy Food (FR6), Budmax (DIY3). *Cluster 3:* BRV Kyiv (DIY1), Nova Linia (DIY2), Epicentr K (DIY4), Furniture Company of Ukraine (DIY6), JYSK Ukraine (DIY7).

Fig. 2. Probability of retailers' online business R_{IT} in 2020 in terms of clusters *Cluster 1* (a), *Cluster 2* (b), *Cluster 3* (c) *(developed by the author)*

Among the set of retailers that formed *Cluster 1*, the results of the calculations identified the status 2 "change" for 2 of 3 studied food retailers – FR1, FR2, 2 drogeries – DR1 and DR2, 4 of 6 retailers in the field of home appliances and electronics – HA1, HA2, HA3, HA5, as well as DIY-retailer – DIY5. It is found that IT risks are very likely for FR1, due to the retailer's rethinking of the need to integrate advanced IT into a compehensive online business management system and increase the cost of their implementation to ensure the congruence of IT and business strategies aimed at maximum satisfaction, needs and preferences of online buyers. For FR2, the probability of risks is due to the design of business processes without focusing on IT, which resist the rapid online business development and increase the risk probability. DR1 scores reflect an advanced IT provisioning and support system using the relevant toolkit, but without investing in IT development and optimizing IT costs. Given the low interest of DR1 in building IT capacity, the status 2 "change" of R_{IT_1} is identified. Unlike DR1, in DR2 the risks in the group R_{IT_1} are higher, which is primarily due to the reluctance to use modern IT for strategic decision-making and online business management based on digital transformation trends.

The score R_{IT_1} of HA1 is explained by inaccuracy in the general system of accounting for the costs of the IT implementation and updating, as well as weak control / lack of control over the implementation of the IT budget. In addition, it can be stated that the retailer HA2 does not have a strategic focus on the IT strategy implementation. As the explanation for the likelihood of HA3 risks might be that when drawing up the operating budget, the retailer has some difficulty in taking into account the total IT cost. The consequence of this is also an incorrect organization of the total management costs. R_{IT_1} risk assessments are shown an incorrect interpretation of HA5 requests, needs and preferences of online buyers regarding IT security and the use of unacceptable authentication settings in the online shop. The status 2 "change" is also identified as a result of the R_{IT_1} assessment for DIY5 included in *Cluster 1*. The prerequisite for this is the setting of tasks in the absence of a well-founded IT strategy, which allowed in a relatively short period of time to achieve the overall goal of online business in the context of digital transformation.

For FR3 it is identified the weak links between mission, vision, understanding of requests, needs, preferences of online buyers and their behavior, staff competence, financial and investment management, business processes and communications at different hierarchical levels. The DIY3 risk status R_{IT_1} is negatively affected by the difficult navigation of the online shop website for online buyers and the low level of IT security when placing online orders, which is partly due to the lack of an identification procedure. In *Cluster 3*, where the status 2 "change" for the risk group R_{IT_1} is identified for 4 DIY retailers. Such DIY1 assessments are due to the inability of staff to identify IT problems in a timely manner and focus their efforts on achieving them. Unlike DIY1, scores of R_{IT_1} in DIY2 and DIY7 are lower and indicate too deep immersion in operational management and the inability to develop and adjust the online business vision, which provides maximum satisfaction of requests, needs and preferences of online buyers through timely implementation of IT solutions. It is worth noting that DIY6 has the highest probability of group risks R_{IT_1}, both among retailers in *Cluster 3* and among other clusters – *Cluster 1*, *Cluster 2*.

It is identified the status 2 "change" for the retailer in the field of home appliances and electronics in *Cluster 1* (HA3) and DIY-retailer in *Cluster 3* (DIY1). The high probability of a risk group R_{IT_2} for HA3 is explained by the development of HR-strategy without the use of grading, which is able to provide an objective assessment of the IT professionals results, their competence, contribution to constructive solutions to online business problems and establish appropriate rewards. The identified risk group status for DIY1 is due to the inability to provide flexible and systematic training of IT professionals with an emphasis on improving their knowledge, skills and abilities in IT, as well as the lack of focus on developing competencies and critical thinking that contribute to the solution of management tasks.

Based on the calculations, the status 2 "change" is identified for the risk group R_{IT_3} for FR4, DR2, HA6 in *Cluster 1*, FR3, FR6, DIY3 in *Cluster 2* and DIY1, DIY4, DIY6, DIY7 in *Cluster 3*. The FR4 score shows a low level of staff motivation to quickly identify and administer cyberincidents, which directly affects the retailer's online business. Another group R_{IT_3} for DR2 in *Cluster 1* is more likely to have group risks due to the occasional use of IT to diagnose and monitor metrics that allow to fragment the online business effectiveness. Partial concentration on promising IT projects to combat cyberattacks and ensure control over IT operations is increased the likelihood of R_{IT_3} for HA6. Changing the identified status for HA6 requires the focus on improving cyberattack protection.

Analyzing the calculation data for retailers in *Cluster 2*, it should be noted that the probability of risks for FR3 is higher than for FR6 and DIY3. This is due to the corporate culture, where the specialists of the IT department are disorganized and work effectively under the mode of "manual" management. Prerequisite for the status 2 "change" for the risk group R_{IT_3} for FR6 – the retailer's reluctance to develop and use in practice personalized applications and IT solutions tailored to the individual needs of online buyers. The

risks of DIY3 in the group R_{IT_3} are high due to the increased dependence on outsourcing and cooperation with business partners which do not seek to improve the quality of service delivery and carry out unsystematic market expansion.

The likelihood of risks R_{IT_3} for DIY1 is due to the lack of a holistic understanding of the IT role in the context of effective IT online business administration. The DIY4 score represents the need to implement mentoring and coaching practices with the collaboration of specialists from different departments on IT projects in order to develop the effective response system to cyberattacks and ensure the appropriate level of further IT support. The identified status 2 "change" for DIY6 is due to the ambiguity of the strategic idea of the retailer's online business, which does not allow the IT department to turn it into a concrete result and, consequently, does not provide the appropriate level of information system administration and IT transformations. Incorrectly established metrics for diagnosing and monitoring the status and effectiveness of IT operations have significantly affected the activities of DIY7 and increased the likelihood of risks R_{IT_3}.

To ensure the sustainable and dynamic development of online business, it is necessary to carry out effective IT risk management. This involves making rational business decisions to implement a set of activities to level or eliminate the risks of online business. That is why, in order to reduce the negative consequences for the conduct and development of online business in the event of risks, the author developed the continuum of unified activities aimed at reducing the negative consequences for the online business conduct and development in the risk R_{IT} groups (Table 1).

The implementation of the proposed relevant activities for leveling and / or liquidation will ensure the adoption of correct management decisions and facilitate the rapid online business scaling.

Table

The continuum of unified activities to reduce the negative consequences from R_{IT} *(developed by the author)*

Group of R_{IT} risks	Activity	Group of R_{IT} risks	Activity
Group 1	Business process automation and IT application to identify differentiated requests, needs and preferences of online buyers	***Group 3***	Improving the mechanism of response to the probable occurrence of cyberincidents on the basis of accumulated data
	Optimization of critical business processes and their standardization		
	Modernization of IT security architecture		
	Rationalization of IT security tools		
	Renovation of technologies for protection against cyberattacks and cyberincidents.		Diagnosis of the level of IT protection against possible cyberattacks and cyberincidents
	Development of the complex operation plan to eliminate the negative consequences of the online business risks, in particular, cyberincidents		
	Increasing the speed in response to cyberattacks and cyberincidents		Designing of business processes to ensure IT security
Group 2	Development and implementation of cybersecurity policy with the involvement of management and competent IT professionals and other employees		Modernization of IT security management system
	Formation and expansion of intelligent databases for assessing the likelihood of risks in the context of effective IT security management		Development of the alternative cyberincident response plans
	Ensuring the flexibility of the IT infrastructure		Risks prediction, including those caused by the growth of cyberattacks and cyberincidents, using intelligent IT security tools
	Ensuring cybersecurity and increasing the level of the online business IT protection		
	Comprehensive verification of the IT security level		
	GAP analysis		

Conclusions and prospects for further research in this area. Based on the results of the detailed analysis of scientists' researchers, the systematized list of three groups of online business IT risks is developed and its graphic interpretation is given. Compared to others, these IT risks take into account the characteristics and impact of digital transformation on online business. The scientific and methodical approach to assessing the probability of IT risks and making correct decisions to level or eliminate them in the future is substantiated. The approbation of the approach is carried out by the example of Ukrainian retailers that have online business in different market segments. The continuum of unified activities to reduce the negative consequences from R_{IT} is developed, based on the results of approbation.

ЛІТЕРАТУРА

1. Артеменко Л. П. Удосконалення процесу управління ризиками у ході впровадження новітніх інформаційних технологій / Л. П. Артеменко, Т. В. Ситник // Молодий вчений. – 2015. – № 1 (1). – С. 38-41.

2. Aven T. Risk assessment and risk management: review of recent advances on their foundation / T. Aven // European Journal of Operational Research. – 2016. – Вип. 253. – № 1. – С. 1-13.

3. Бавико О. Є. Синхронізація розвитку ринку інформаційно-комунікаційних технологій в Україні з глобальними трендами / О. Є. Бавико // Маркетинг і менеджмент інновацій. – 2018. – № 1. – С. 272-283.

4. Forsythe S. M. Consumer patronage and risk perceptions in Internet shopping / S. M. Forsythe // Journal of Business Research. – 2003. – Вип. 56. – № 11. – С. 867-875.

5. Hao X. IT Operational risk measurement model based on internal loss data of banks / X. Hao // E-business Technology and Strategy, CETS 2010, Communications in Computer and Information Science. – 2010. – Вип. 113. – С. 180-191.

6. Lisanti Y. IT service and risk management implementation for online startup SME: Case study: Online startup SME in Jakarta / Y. Lisanti, D. Luhukay, V. Mariani // International Conference on Information Management and Technology (ICIMTech). – 2017. – С. 300-303.

7. Milne G. R. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices / G. R. Milne, M. J. Culnan // Journal of Interactive Marketing. – 2004. – Вип. 18. – № 3. – С. 15-29.

8. Natorina A. Online retailers' management system of marketing commodity policy / A. Natorina // Economic Annals-XXI. – 2018. – № 174 (9-10). – С. 69-72.

9. Наторіна А. О. Маркетингова товарна політика онлайн-ритейлерів: характеристика та траєкторії розвитку / А. О. Наторіна // Бізнес Інформ. – 2018. – № 9. – С. 272-277. URL: https://www.business-inform.net/export_pdf/business-inform-2018-9_0-pages-272_277.pdf (дата звернення: 05.05.2020).

10. Obrand L. The interstitiality of IT risk: an inquiry into information systems development practices / L. Obrand, N-P. Augustsson, L. Mathiassen, J. Holmstrom // Info Systems. – 2019. – № 29. – С. 97-118.

11. Скопенко Н. С. Особливості формування комплексної системи ризик-менеджменту / Н. С. Скопенко // Теоретичні та прикладні питання економіки. – 2016. – Вип. 1. – С. 32-42.

12. Teymouri M. The impact of information technology on risk management / M. Teymouri, M. Ashoori // Procedia Computer Science. – 2011. – Вип. 3. – С. 1602-1608.

13. Tohidi H. The role of risk management in IT systems of organizations / H. Tohidi // Procedia Computer Science. – 2011. – Вип. 3. – С. 881-887.

14. Yermak S. Problems of innovative activity development at food industry enterprises of Ukraine / S. Yermak // Journal of Hygienic Engineering and Design. – 2017. – Вип. 21. – С. 96-102. URL: http://www.jhed.mk/filemanager/JHED%20Vol.%2021/03.%20FPP/09.%20Full%20paper%20-%20Svitlana%20Yermak.pdf (дата звернення: 04.05.2020).

REFERENCES

1. Artemenko, L. P. and Sytnyk, T. V. (2015), Udoskonalennia protsesu upravlinnia ryzykamy u khodi vprovadzhennia novitnikh informatsijnykh tekhnolohij, *Molodyj vchenyj*, № 1 (1), s. 38-41.

2. Aven, T. (2016), Risk assessment and risk management: review of recent advances on their foundation, *European Journal of Operational Research*, vol. 253, no. 1, pp. 1-13.

3. Bavyko, O. Ye. (2018), Synkhronizatsiia rozvytku rynku informatsijno-komunikatsijnykh tekhnolohij v Ukraini z hlobal'nymy trendamy, *Marketynh i menedzhment innovatsij*, № 1, s. 272-283.

4. Forsythe, S. M. (2003), Consumer patronage and risk perceptions in Internet shopping, *Journal of Business Research*, vol. 56, no 11, pp. 867-875.

5. Hao, X. (2010), IT operational risk measurement model based on internal loss data of banks, *E-business Technology and Strategy*, CETS 2010, Communications in Computer and Information Science, vol 113, pp 180-191.

6. Lisanti, Y., Luhukay, D. and Mariani, V. (2017), IT service and risk management implementation for online startup SME: Case study: Online startup SME in Jakarta, *International Conference on Information Management and Technology (ICIMTech)*, pp. 300-303.

7. Milne, G. R. and Culnan, M. J. (2004), Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices, *Journal of Interactive Marketing*, vol. 18, no. 3, pp. 15-29.

8. Natorina, A. (2018), Online retailers' management system of marketing commodity policy, *Economic Annals-XXI*, no. 174 (9-10), pp. 69-72.

9. Natorina, A. O. (2018), Marketynhova tovarna polityka onlajn-rytejleriv: kharakterystyka ta traiektorii rozvytku, *Biznes Inform*, № 9, с. 272-277, available at: https://www.business-inform.net/export_pdf/business-inform-2018-9_0-pages-272_277.pdf (data zvernennia: 05.05.2020).

10. Obrand, L., Augustsson, N-P., Mathiassen, L. and Holmstrom, J. (2019), The interstitiality of IT risk: an inquiry into information systems development practices, *Info Systems*, no. 29, pp. 97-118.

11. Skopenko, N. S. (2016), Osoblyvosti formuvannia kompleksnoi systemy ryzyk-menedzhmentu, *Teoretychni ta prykladni pytannia ekonomiky*, vyp. 1, s. 32-42.

12. Teymouri, M. and Ashoori, M. (2011), The impact of information technology on risk management, *Procedia Computer Science*, vol. 3, pp. 1602-1608.

13. Tohidi, H. (2011), The role of risk management in IT systems of organizations, *Procedia Computer Science*, vol. 3, pp. 881-887.

14. Yermak, S. (2017), Problems of innovative activity development at food industry enterprises of Ukraine, *Journal of Hygienic Engineering and Design*, vol. 21, pp. 96-102, available at: http://www.jhed.mk/filemanager/JHED%20Vol.%2021/03.%20FPP/09.%20Full%20paper%20-%20Svitlana%20Yermak.pdf (accessed 4 May 2020).

Стаття надійшла до редакції 08 травня 2020 року