Economic Affairs, Vol. 67, No. 04, pp. 619-629, September 2022
DOI: 10.46852/0424-2513.4.2022.28

AESSRA

Review Paper

Economic Security of the Enterprise Within the Conditions of Digital Transformation

Yuliia Samoilenko[1]*, Igor Britchenko[2], Iaroslava Levchenko[3], Peter Lošonczi[4], Oleksandr Bilichenko[5] and Olena Bodnar[6]

[1]Department of Software Engineering and Cybersecurity, Kyiv National University of Trade and Economics, Kyiv, Ukraine
[2]Department of Finance, Higher School of Insurance and Finance (VUZF), Sofia, Bulgaria
[3]Department of Economics and Entrepreneurship, Kharkiv National Automobile and Highway University, Kharkiv, Ukraine
[4]Department of Economic Sciences, Vice-rector for Scientific Work and Educational Process, University of Security Management in Košice, Slovakia
[5]Department of Economic Theory and Social Sciences, Mykolayiv National Agrarian University, Mykolayiv, Ukraine
[6]Department of Finance, Banking and Insurance, Mykolayiv National Agrarian University, Mykolayiv, Ukraine

*Corresponding author: juliyasamoil@gmail.com (**ORCID ID:** 0000-0003-3787-1435)

Received: 13-05-2022 **Revised:** 30-08-2022 **Accepted:** 08-09-2022

ABSTRACT

In the context of the digital economy development, the priority component of the economic security of an enterprise is changing from material to digital, constituting an independent element of enterprise security. The relevance of the present research is driven by the need to solve the issue of modernizing the economic security of the enterprise taking into account the new risks and opportunities of digitalization. The purpose of the academic paper lies in identifying the features of preventing internal and external negative influences (threats) in order to guarantee the effective and stable functioning and dynamic social development of the enterprise in the context of digitalization. The research methods are as follows: general scientific research methods, in particular, logical analysis, theoretical substantiation, methods of induction and deduction, formalization and generalization, statistical observation. Results. It has been proposed to introduce the concept of "digital security of the enterprise" for replacing the concept of "information component of economic security" in order to bring the terminology in line with new economic realities. The implementation of the "black box" model has made it possible to identify the latest risks and threats to the economic security of an enterprise within the conditions of the digitalization that differs from the existing ones. The assessment of enterprises' digital security of the European Union member states has revealed that the digital security level does not depend on the size of the country, however, it is influenced by the institutional environment (in particular, digital development tools in the EU) and the size of enterprises. Also, within the research framework, an assessment of the digital security level of enterprises in the context of digitalization has been proposed. In order to characterize enterprises by the level of digital security, a calculation procedure using the coefficient method has been proposed.

HIGHLIGHTS

- The economic security of the enterprise in the conditions of digital transformation is a priority component of the economic security of the enterprise;
- Resolved issues of modernization of the enterprise' 's economic security, taking into account new risks and possibilities of digitalization.

Keywords: Digital economy, economic security of the enterprise, information security, digital security of the enterprise, threats, risks, digitalization, EU

How to cite this article: Samoilenko, Y., Britchenko, I., Levchenko, I., Lošonczi, P., Bilichenko, O. and Bodnar, O. (2022). Economic Security of the Enterprise Within the Conditions of Digital Transformation. *Econ. Aff.*, **67**(04): 619-629.

Source of Support: None; **Conflict of Interest:** None

Solving the issues of ensuring economic security in the modern realities of digitalization of social-economic processes is an essential, and urgent goal for the national economy. Unsteady external and internal conditions, digital transformation of almost all spheres of life inevitably give rise to new threats and challenges, requiring a prompt response and improvement of ways to minimize risks.

The accumulated experience provides an opportunity to state that economic security is a key characteristic for the stable functioning and achievement of the necessary development indicators for both individual business entities and society as a whole. Security of economic processes is characterized by numerous political, legal, and economic mechanisms and tools that help protect economic interests. In a broad sense, economic security can be considered as the ability of the institutional and organizational system to protect the interests of economic entities based on international and national legal norms concerning and observance of national traditions and values of management. Innovative information and computer technologies, constituting the basis of the digital economy, play a significant role in developing all aspects of society. Digitalization processes have a particularly significant impact on the economic activities of business entities and, consequently, on ensuring their economic security.

Despite the close attention to the problems of digitalization on the part of numerous investigations, the issues of the influence of digital technologies on the economic security of enterprises have been studied and elaborated insufficiently.

Business responds best to changes in the external environment; therefore, in the context of solid uncertainty, due to the digital transformation of society, it can act as an essential tool in matters of its sustainable development. One of the key features of 2020 was the active digitalization of various sectors of the economy during the COVID-19 pandemic. Taking into consideration the complex epidemiological situation and the transition of many organizations to a remote working mode, the level of digitalization of enterprises is becoming more relevant than ever. This has entailed a significant increase in requirements for data transmission speed, the quality of digital services provided, their availability for customers, and the economic security of enterprises. The obvious fact is that the reduction of restrictive measures will not lead to a rejection of further digitalization of enterprises; therefore, the emphasis on developing and providing economic security of enterprises, on the contrary, from the point of view of the outlined trends, will remain. For all the reasons outlined, the issue of ensuring enterprises' required level of economic security and the formation of a functioning system for identifying, assessing, and minimizing information risks is relevant.

Literature Review

The demand for security is fundamental for individuals, enterprises, society, and the state as a whole. Some scholars have focused on national economic security (Buzan, Hansen, 2009), the economic security of households (Dynan, 2016), and the economic security of the individual (Hacker *et al.* 2014). Others have paid attention, in addition to the above, to "economic security of the region and economic security of the enterprise" (Shutiak *et al.* 2014). Thus, at all stages of economic development, economic security is a critical element of the economy and demands protection from internal and external threats.

The analysis of the conceptual apparatus of the enterprise's economic security has shown that this concept is considered from several points of view as follows (Ianioglo, Polajeva, 2016):

1. Protection against threats (protection of scientific and technical, production and personnel potential of the enterprise) from active or passive economic threats. Hazard is "a source of danger that could harm an asset" (Rausand 2011). Threats to the economic security of the enterprise are potential or actual actions of individuals or legal entities that may lead to economic or other losses up to the bankruptcy of the enterprise. "The concept of threat is closely related to the concept of danger; however, it differs from it by the fact that the latter is not aimed at exploiting vulnerabilities. After all, a threat is a danger, but danger is not necessarily a threat" (Rausand 2011). These are main threats to the external environment. It is essential to find the optimal balance between the probable losses in cases of violation of the enterprise's interests and the acceptable

cost in order to avoid or minimize losses (Suglobov *et al.* 2013);

2. State of efficient use of resources. Economic security ensures stable operation and dynamic scientific, technical, and social development of the enterprise; it prevents internal and external negative impacts (threats) through the most efficient use of corporate resources (capital, personnel, information, technology and engineering, equipment, legal resources) and business opportunities (Pokropyvnyi, 2006; Ianioglo, Parmacli, 2015). However, the economic security of the enterprise is considered from an overinclusive point of view and, in fact, is identified with the activities and efficiency of the enterprise, which, in our opinion, is not entirely true;
3. The ability to stable functioning and development. The economic security of the enterprise lies in ensuring the stability of economic activity during each cycle of production, exchange, distribution, and consumption and neutralization of factors undermining the stable functioning of the economic mechanism of the enterprise (Ioan-Franc, Diamescu, 2010). The economic security of the enterprise should not be limited to neutralizing factors; however, it should provide constant protection. By the term under consideration, the authors understand the state of the economic, legal, and industrial relations of the enterprise, as well as material, intellectual, and information resources, expressing the ability of the enterprise towards stable functioning. The primary focus is on ensuring the stable operation of the enterprise. Herewith, it is important not only to ensure stability but also to support the development of the enterprise;
4. Availability of competitive advantage. Suglobov *et al.* (2013) believe that economic security is a system providing competitive advantages to the enterprise through the efficient use of resources (material, labor, financial, investment) based on the complex studying information generated in an integrated accounting and information system. In the process of ensuring economic security, the author attaches particular importance to information that, if used correctly, can provide benefits to the company;
5. Achieving the target goals as a criterion of economic security (Zigunova *et al.* 2020), which characterizes the state of the enterprise based on the assessment of its ability to function correctly to accomplish the desired goals under existing external conditions and their change within certain limits. While the first approach assumes that the enterprise is economically safe when it is protected from threats, then according to the fifth approach, ensuring economic security is a more difficult task of providing the enterprise with such qualities with which it can achieve business goals. In contrast to the first approach, activities on ensuring the economic security of the enterprise are transferred to the analytical and management level.

The economic security of the enterprise is one of the elements of national security protection (Korchevska, 2015). Strelcova *et al.* (2015) believe that economic security is a state in which an entity (enterprise, country, group of countries, world, person, family, etc.) is protected insomuch that it is not exposed to threats that can significantly reduce its efficiency, necessary for ensuring defense, as well as competitiveness in the domestic and foreign markets. The authors consider economic security from the standpoint of protection against threats and maintaining the competitiveness of the business entity.

Liubokhynets *et al.* (2020) have investigated minimizing the negative impact of destabilizing factors on economic security, which leads to the need to apply various approaches and methods that allow companies to successfully and steadily develop.

The economic security of the enterprise, in particular, the formation of its supporting system, depends on changes in external and internal environments. Nowadays, it is the development of the digital economy and the COVID-19 pandemic.

Lipych, and Skoruk (2020), figuring out the essence and features of the digital economy, established that Denmark, Sweden, and Finland have taken the leading positions in the digital economy over the past three years; the lowest level of digitization has

been observed in Bulgaria, Romania, and Greece. The authors determine the need to develop and implement a system of financial and economic security of an enterprise in the context of the digital economy development and the conditions of digitalization as a necessary element of the enterprise's internal economic mechanism for both protection of activity against external and internal negative factors and introduction of innovative information technologies and the software for its stable and dynamic development.

The investigations in the field of economic security of the enterprise within the conditions of digital transformations mainly cover the topics as follows: the impact of information and communication technologies (from now on – ICT) on the conduct of business enterprises, increasing their efficiency and competitiveness (Real, Leal & Roldán, 2006), the impact of ICT on economic growth and development (Stankic, Jovanovic Gavrilovic & Soldic Aleksic, 2018), on the economy and the society as a whole (Roztocki, Soja & Weistroffer, 2019). Bouwman, van der Hooff, van der Wijngaert & van Dijk (2005) analyze the adoption, implementation, application, and consequences of using ICT in various organizations. Studies concern the impact of ICT on enterprises' activities; however, the impact of digital transformations on the economic security of enterprises is underrepresented in scientific investigations. Recent explorations are devoted to implementing the latest information systems technologies, such as cloud computing and rich data analytics. The most important concepts and features of big data are discussed in the scientific work (Chroneos-Krasavac, Soldic-Aleksic & Petkovic, 2016).

Kazmin *et al.* (2020) consider the security of information circulating in economic information systems. Based on the system analysis of technical channels of information leakage and methods of unauthorized access, a list of typical unauthorized malicious actions against economic information systems, as well as technical channels of information leakage when intercepting confidential information contained in economic information systems, is presented. The results of the analysis have made it possible for scientists to clarify measures towards ensuring the confidentiality, integrity, and accessibility of information circulating in economic information systems based on modern information technologies.

Gaspareniene *et al.* (2016), considering the threats to the development of the digital economy, specify the drivers of digital shadow consumption that are identified as separate threats. Kadar *et al.* (2014) note that increased competition is accompanied by increased current threats and dangers and the emergence of new ones. The management of any enterprise should be aware of this. However, the study of the human factor in digitalization security processes narrows down to the implementation of information security (Khan *et al.* 2011). Scholz (2017) focuses on digitalization, legal zones, etc.; along with this, the scholar does not consider the need for digital security in the enterprise.

The academic paper aims to identify the features of preventing internal and external negative influences (threats) to guarantee the effective and stable functioning and dynamic social development of the enterprise within the conditions of digitalization.

MATERIALS AND METHODS

The research methods are as follows: general scientific research methods, in particular, logical analysis, theoretical substantiation, induction and deduction, formalization and generalization, and statistical observation.

The results of the research are based on EU and OECD statistics. Concerning the investigations of ICT use in EU countries, the data source is the European Digital Progress Report (EDPR), containing a digital profile of each country (Country Profile), and it is published annually by the European Commission; data of the statistical study "The use of information and communication technologies (ICT) in enterprises", the results of which are published on the Eurostat website in the section "Digital Economy and Society".

Because EU member states differ significantly in their digitalization features, in particular, the research is based on the hypothesis that differences between EU member states, reflecting all aspects of their use of information and communication technologies, affect the digital security of enterprises.

RESULTS

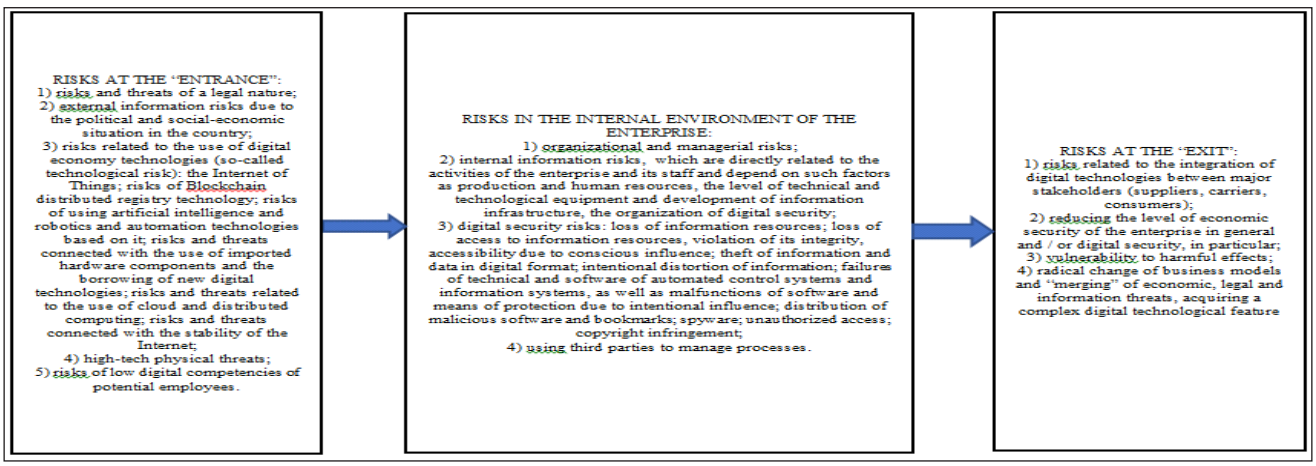
Ensuring the economic security of an enterprise is

important for the implementation of a continuous reproduction process. The economic security of the enterprise includes three important elements, namely: economic independence, sustainability and development. Economic independence involves fulfilling control over one's own resources; it is the ability to pay one's obligations on time. It is necessary to obtain such production level to ensure the enterprise's competitiveness in the market. Sustainability is understood as the stability of functioning, the financial situation in which the fulfillment of all its obligations to employees, other organizations, and the state is ensured. Development involves increasing the efficiency of the enterprise and bringing it to a satisfactory condition. In case the enterprise neither develops nor achieves efficiency, then its ability to adapt to external and internal conditions decreases, and, therefore, the survival rate decreases. Consequently, enterprises are in a state of constant improvement in order to achieve and maintain a level of economic security.

We are of the opinion that the process of digital transformation lies in shifting the emphasis from tangible assets to intangible (digital, virtual), automation of business processes through the introduction of modern information (digital) technologies and systems, and creating new business models based on them. The entire complex of information, objects of informatization, information (digital) technologies and systems, the introduction of ICT, and the transition of an enterprise to functioning in a digital environment bear new risks and threats that are not characteristic of traditional (non-digital) processes (Fig. 1). Ensuring economic security, in point of fact, comes down to the pairing of these threats. Therefore, the organization of activities to ensure the economic security of enterprises to a great extent depending on the method of their identification and classification.

Actually, in economic science, the concept of economic security of an enterprise is considered as a set of components, among which information is distinguished as information protection; that is, it is connected with the processes of informatization of the enterprise's activities, which in modern conditions have taken the form of digitalization, as well as with the protection of information resources. In this regard, ensuring the economic security of the enterprise has been built only in the form of an information protection system. Therefore, taking into account the modern conditions of digital transformation, it is advisable to introduce the digital security of the enterprise as a state of digitalization in economic science, instead of information one, ensuring the economic and informational interests of the enterprise in the current period and its strategic economic security in the long term based on appropriate technologies to the current state of the industrial revolution (in this context – Industry 4.0).

Consequently, ensuring economic security in the context of digitalization should be based on digital security – that is, the formation of qualitatively new factors contributing to the participation of enterprises in a unified information system for



Source: *Developed by the author.*

Fig. 1: Types of risks and threats in the context of digitalization of enterprises according to the model of the "Black Box"

ensuring the economic security of enterprises and reducing external and internal risks.

Digital transformation differs from automation and informatization in the fact that it requires systemic changes in business processes, business models, and economic relations, both within and around the enterprise. Creating an environment for the digital transformation of enterprises operating in traditional sectors of the economy should include a range of specialized technology and business consultations that can be conducted by the relevant competence centers. There is also a demand for public-private collaboration on nationwide initiatives (that is, skills development and common standards) and a comprehensive financial framework in order to support enterprises. In particular, the EU has introduced the tools to increase the digital security of enterprises as follows:

- EU sectoral initiative "Digitalization of European Industry" (DEI) in the framework of the "Single Digital Market" package since 2016 and its implementation at the supranational and national levels – Communication from the Commission to the European Parliament, the Council, the European Economic, and Social Committee and the Committee of the Regions: Digitising European Industry Reaping the full benefits of a Digital Single Market (COM (2016);
- Financing of digital transformation for small and medium enterprises (SMEs). At EU level COSME (2014–2020), the EU SME Competitiveness Program provides the COSME Loan Guarantee Facility (LGF), which supports the financing of SME digital transformation projects in all sectors of the economy;
- Regulation (EU) № 1287/2013 of the European Parliament and of the Council as of December 11, 2013 establishing the Programme for the Competitiveness of Enterprises and small and medium-sized enterprises (COSME) (2014–2020) and repealing Decision № 1639/2006/EU. In 2021 – the establishment of the Fund for Recovery and Sustainability (Recovery and Resilience Fund);
- The existence of a central body for policy development for the digital transformation of enterprises in the EU member states;
- A network of Digital Innovation Centers (DIC – European Digital Innovation Hubs (EDIHs));
- Financial package for the program "Digital Europe" for the period 2021–2027 (Regulation (EU) 2021/694 of the European Parliament and of the Council as of April 29, 2021, establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240), as well as a special definition for European Digital Innovation Hubs (EDIHs) has been introduced for transparent allocation of funds;
- Functioning of the European Institute for Innovation and Technology (EIT), including EIT Digital, the leading European organization for digital innovation and entrepreneurship education, which is the driving force behind European digital transformation;
- Digital industrial platforms facilitating the digital transformation of enterprises, in particular, the network of European Digital Innovation Hubs;
- Plan "Digital Compass-2030" (Digital Compass);
- Implementation of the National Broadband Plan (National Broadband Plans) – Communication from the Commission – EU Guidelines for the application of State aid rules in relation to the rapid deployment of broadband networks;
- A particular website "Digital Economy and Society – Overview" (Digital economy and society – Overview);
- The program "Path to the Digital Decade" (The Path to the Digital Decade) - Communication: "2030 Digital Compass: the European way for the Digital Decade".

We propose to analyze the situation in the European Union in order to form a correct viewpoint. In particular, this applies to companies assessing digital security risks, informing their employees of digital security obligations, conducting security tests or regular backups, and also insuring against digital security incidents.

For instance, the European Commission annually publishes the results of the Digital Economy and Society Index (DESI), tracking Europe's overall digital performance and monitoring EU countries' progress in terms of their digital competitiveness. According to Eurostat 2021 (The Digital Economy

Table 1: Digital security of EU enterprises in 2019, %

Countries	Uses at least one ICT security measure	Has documents on ICT security measures, practices or procedures	Documents on enterprise ICT protection have been identified or revised in the last 12 months	Informs employees about their obligations in the field of ICT security	Suffered from ICT-related incidents in 2018	Has insurance against ICT-related incidents	Digital security
EU-27	92	33	24	61	13	21	30,58
Belgium	94	34	27	57	22	25	33,19
Bulgaria	85	18	13	51	16	3	37,20
The Czech Republic	94	32	26	76	21	8	51,40
Denmark	97	56	42	70	10	56	66,20
Germany	97	37	27	68	11	20	52,00
Estonia	86	27	18	55	8	7	40,20
Ireland	93	54	42	76	18	39	64,40
Greece	74	15	10	33	7	25	32,80
Spain	92	33	25	54	12	33	49,80
France	94	26	18	55	15	39	49,40
Croatia	90	41	25	47	19	7	45,80
Italy	93	34	28	73	10	13	50,20
Cyprus	83	32	24	59	11	13	44,40
Latvia	98	42	25	68	12	12	51,40
Lithuania	93	36	22	67	16	4	47,60
Luxembourg	93	27	22	52	17	26	47,40
Hungary	86	17	13	48	15	4	36,60
Malta	92	32	25	59	24	29	52,20
The Netherlands	96	42	32	56	11	26	52,60
Austria	91	36	28	63	12	18	49,60
Poland	87	23	18	49	13	11	40,20
Portugal	98	28	21	54	8	10	43,80
Romania	73	17	11	49	11	5	33,20
Slovenia	84	35	26	53	14	4	43,20
Slovakia	90	28	22	64	15	8	45,40
Finland	97	44	35	66	18	28	57,60
Sweden	95	52	39	66	35	39	65,20

Source: *Summarized and complied by the author based on data of Eurostat https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ra/default/table?lang=en*

and Society Index (DESI) (2021)), Finland, Sweden, Denmark and the Netherlands are the leaders in overall digital productivity in the EU.

The International Digital Economy and Society Index (I-DESI) shows that the above-mentioned EU countries are also world leaders. In order to achieve the Digital Compass 2030 target, at least 90 % of SMEs in the EU should possess a basic level of digital intensity. In 2020, only 60 % of SMEs were at this level in terms of introducing digital technologies (OECD, 2021). Denmark and Finland are already very close to the EU target of 88 %, while Bulgaria and Romania lag far behind (33 %). The digital compass aims for at least 75 % of companies to use artificial intelligence, cloud, and big data technologies by 2030. Businesses are increasingly digitalizing; however, the use of advanced digital technologies remains low. Only one in four companies uses cloud computing and 14 % of big data.

Taking into consideration the multifactority and multidimensional nature of the digital security concept of the enterprise, it may be appropriate to consider the lack of a single definition and recognize the possibility of different interpretations of this concept. Herewith, another problem arises in this case: this diversity of concepts gives rise to a variety of methodological approaches to determining the digital security of enterprises. By the way, the assessment of the digital security of the enterprise

should be mentioned, the level of which is a relative indicator reflecting the state of digitalization, which makes it possible to ensure the economy of the enterprise, measured in a certain period.

For the convenience and value of its practical use, the methodological approach should meet a number of requirements as follows:

- To reflect the key factors of digital transformation in the context of modern economic conditions;
- To provide the simplicity of calculations and economic interpretation of the obtained estimation values;
- Not to cause difficulties regarding the values of individual indicators that are included in the final indicator;
- To exclude excessive subjectivism in the calculated values.

Focusing on fulfilling the above requirements for assessing the digital security of enterprises, one can use the coefficient method of assessment. Its essence lies in calculating specific indicators characterizing the effectiveness of the applying elements of digitalization of enterprises. In this case, the final indicator comes as the arithmetic means of relevant coefficients. According to this approach, the digital security indicators of enterprises in EU member states are calculated. In this case, one can use the indicators of statistical bodies (in the EU – Eurostat "ICT security in enterprises") (Table 1) at the level of enterprises in the country. According to data in 2019, 92 % of EU enterprises with 10 or more employees have used at least one measure in order to ensure the integrity, reliability, accessibility, and confidentiality of ICT data and systems. According to the integral assessment of enterprises' digital security based on the coefficient method, the best positions are taken by enterprises in Denmark, Sweden, Ireland, Finland and the Netherlands, relatively small economies in the EU.

Digital security risk assessment – a periodic assessment of the probability and consequences of digital security incidents; it is the basis for digital security risk management (OECD, 2015) (Table 2).

In the European Union, according to the OECD data based on Eurostat, methods for assessing digital security risks for enterprises are closely correlated with security tests or backup procedures. In general, it can be concluded that large companies carry out this activity on average much more often than small ones. In the EU member states, a significant proportion of large companies perform backups, which are independent of risk assessment practices. In contrast, in countries where a large proportion of small and medium-sized enterprises (from now on referred to as SMEs) carry out risk assessments, a significant proportion of SMEs also introduce backups. This goes to prove that backup in large companies is part of the mainstream of digital security, while in SMEs it is more dependent on risk assessment practices.

In general, the tendency towards insurance can be seen as a sign of the company's serious attitude to digital security. However, it also depends on the

Table 2: Features of digital security risk assessment of EU enterprises

Indicator	State
Proportion of companies conducting assessment of digital security risks	From 14 % in Hungary to 60 % in Finland. The rate increases with increasing company size (less than 1/3 among small companies, approaching 3/4 among large).
Risk transfer (insurance)	From 4 % in Lithuania to over 56 % in Denmark. In all EU countries, except two, the propensity to transfer risk increases with the size of enterprises. In Denmark, it is significantly higher among small enterprises (57 %) compared to medium-sized enterprises (5 %) and large enterprises (40 %). This is also revealed in Slovenia, although to a much lesser extent
Proportion of enterprises that employ people who are aware of their ICT security obligations	It ranges from 1/3 in Greece to more than 3/4 in Ireland, where there is also a high concentration of business in the ICT sector. This share also increases with the size of enterprises: less than 60 % among small enterprises, but more than 90% among large ones

Source: *Summarized and complied by the author according to OECD based on Eurostat (2019), Digital Economy and Society Statistics, Comprehensive Database StatLink https://doi.org/10.1787/888934192357; Eurostat (2019), Digital Economy and Society Statistics, Comprehensive Database.); OECD based on Eurostat (2019, Digital Economy and Society Statistics, Comprehensive Database. StatLink https://doi.org/10.1787/888934192376.*

availability of insurance policies in the country covering the risk of digital security. Traditional insurance policies or individual cyber insurance policies can cover risks. Consequently, some companies may think that traditional policies apply to them, but this is not the case (OECD, 2020).

Therefore, all of the indicators mentioned above, based on Eurostat data, clearly show that the tendency of enterprises toward implementing digital security measures increases with their size.

DISCUSSION

The study has confirmed the research hypothesis that differences between member countries affect the level achieved in the introduction and implementation of information and communication technologies in enterprises of EU countries. In several studies on the use of ICT in enterprises in European countries, efforts have been made to rank countries by their level of adoption and identify factors influencing the ICT adoption process. J. Becker, A. Becker, P. Sulikowski, and T. Zdziebko (2018) rank the countries of Central Europe as members of the European Union (Austria, the Czech Republic, Germany, Hungary, Slovakia, Slovenia) based on the application of ICT in enterprises that use analytical networking process (ANP). The survey revealed that among these countries, Slovenia and Austria were the leaders in 2017 in using ICT in enterprises. A. Zečević and J. Radović-Stojanović (2018) analyzed the use of ICT in enterprises in Slovenia, Croatia, the Republic of Serbia, Bosnia and Herzegovina, Macedonia, and Montenegro. They have noted that investment and development of information and communication infrastructure are factors influencing the use of ICT in enterprises of these countries. In the course of the research, the conclusion has been made that EU member states, namely Slovenia and Croatia, are leading in the use of ICTs in their enterprises, especially in the implementation of advanced technologies, that is, cloud computing and e-commerce. However, our research indicates that this situation changed in 2020, and the EU countries are increasing the digitalization of enterprises, which has a positive effect on their economic security.

CONCLUSION

The introduction of digital technologies into the business processes of enterprises bears new risks and threats that are not characteristic of traditional (non-digital) processes; they are caused by new technologies and features of the digital economy. Identifying possible risks and threats is one of the most important goals in ensuring the economic security of the enterprise in the context of the digital economy. The efficiency of the developed and applied measures towards minimizing risks and neutralizing threats to the economic security of an enterprise depends on the quality and timeliness of the goal outlined. The approach to the analysis of risks and threats of the enterprise in the digital economy should be complex; it should cover all basic business processes of the enterprise both in the internal and external environment.

An assessment of the enterprises' digital security in the EU member states has shown that small and dynamic European economies, in particular, are characterized by higher security indicators in the context of digitalization; they are the ones that achieve the best indicators in the implementation of ICT. They are looking for opportunities to develop ICT and often surpass large countries with advanced economies in terms of the application of digital security in enterprises.

The level of achieved economic security is an essential factor due to the volume of investments in information technology, the development of an information business culture, and the desire of enterprises to introduce modern ICT.

The level of economic security also influences the adoption of advanced information technologies such as cloud computing and e-business integration in enterprises. Additional investigations are required to clarify the influence of these factors and the possible identification of other factors affecting the digital security of enterprises. In particular, the issue of the impact of the regional situation of countries on the enterprises' digital security warrants further study. Along with this, the subsequent directions of studying can be the development of methodological fundamentals for determining the level of digital security of an enterprise based on a system of indicators, in particular, the use of digital marketing, analysis of work in remote mode, and the use of digital economy technologies.

REFERENCES

Arhireyska, N.V. 2013. Doslidzhennya sistemnih pidhodiv schodo otscinki kategorii "ekonomichna bezpeka" [study of systemic approaches to the assessment of the category of "economic security"]. Efficient economy, 8. Retrieved from: http://www.economy.nayka.com.ua/?op=1&z=2235. (in Ukranian).

Becker, J., Becker, A., Sulikowski, P. and Zdziebko, T. 2018. ANP-based analysis of ICT usage in Central European enterprises. Paper presented at the 22nd International Conference on Knowledge-Based and Intelligent Information, & Engineering Systems. *Procedia Computer Science,* **126**: 2173–2183.

Bouwman, H., van der Hooff, B., van der Wijngaert, L. and van Dijk, J. 2005. Information and Communication Technology in Organizations: Adoption, Implementation, Use and Effects. Amsterdam, NI: Boom.

Buzan, B. and Hansen, L. 2009. The evolution of international security studies. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511817762.

Chroneos-Krasavac, B., Soldic Aleksic, J. and Petkovic, G. 2016. The big data phenomenon: The business and public impact. *Industrija,* **44**(2): 117–144.

Dynan, K.E. 2016. Household economic security and public policy, *Business Econ.,* **51**(2): 83–89.

Ekonomika pidpryiemstva [Business Economics] 2006. Za red. S. F. Pokropyvnoho. – K.: KNEU. pp. 528 (in Ukranian).

European Investment Bank, 2019. Financing the digitalisation of small and medium-sized enterprises The enabling role of digital innovation hubs https://www.eib.org/attachments/thematic/financing_the_digitalisation_of_smes_summary_en.pdf.

Eurostat, 2021. Digital Economy and Society Statistics, Comprehensive Database.) Retrieved from: https://ec.europa.eu/eurostat/web/digital-economy-and-society.

Eurostat, 2021. Security incidents and consequences Retrieved from: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ic/default/table?lang=en.

Eurostat, 2021. Security policy: measures, risks and staff awareness Retrieved from: https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ra/default/table?lang=en. https://ec.europa.eu/eurostat/databrowser/view/isoc_cisce_ic/default/table?lang=en.

Gaspareniene, L., Remeikiene Remeikiene, R. and Schneider, F.G. 2016. The factors of digital shadow consumption, *Intellectual Economucs,* **9**: 108. 108–119.

Hacker, J.S., Huber, G.A., Nichols, A., Rehm, P., Schlesinger, M., Valletta, R. and Craig, S. 2014. Economic security index: a new measure for research and policy analysis, *Review of Income and Wealth,* **60**(S1): 5–32.

Ianioglo, A.I. and Parmacli, D.M. 2015. Effektivnost' zemlepol'zovaniya i ehkonomicheskaya bezopasnost' sel'skohozyajstvennyh predpriyatij [Land use efficiency and economic security of enterprises], Chapter 6, in D. M. Parmacli, *et al.* Jeffektivnost' zemlepol' zovanija: teorija, metodika, praktika: monografija. Gos. un-t, Nauch.-issled. centr "Progress". Komrat: B. I. (in Russian).

Ianioglo, A. and Polajeva, T. 2016. Origin and definition of the category of economic security of enterprise, in 9th International Scientific Conference proceedings "Business and Management 2016", 12–13 May 2016, Vilnius, Lituania, 1–8. https://doi.org/10.3846/bm.2016.46.

Illiashenko, O.V. 2016. Mechanisms of the system of economic security of the enterprise / Kharkiv: Machulin, 503 p. (in Ukranian).

Ioan-Franc, V. and Diamescu, M.A. 2010. Some opinions on the relation between security economy and economic security, *Romanian J. of Econ.,* **31**: 129–159.

Kadar, M., Moise, I.A. and Colomba, C. 2014. Innovation management in the globalized society, *Procedia – Social and Behavioral Sciences,* **143**: 1083–1089.

Kavun, S.V. 2009. The system of economic security: methodological and methodological principles: monograph, Kharkiv: KhNEU, 300 p. (in Ukranian).

Kazmina, I., Shafranskaya, C., Saenko, I. Kozhemov, S., Gayazova, S. and Zatsarinnaya, E. 2020. *An Economic Security Management System of an Enterprise in the Digital Economy,* **12**(3s) : Special Issue.

Khan, B., Alghat Alghathbar, K.S., Nabi, S.I. and Khan, M.K. 2011. Effectiveness of information security awareness methods based on psychological theories, *African J. of Business Manag.,* **5**(26): 10862–10868.

Korchevska, L. 2015. Periodization of the stages of the formation and development of knowledge about economic security of enterprise, *Wspolpraca Europejska/ European Cooperation,* **1**(1): 54–65.

Kozachenko and Hkh, V. 2015. Ekonomichna bezpeka pidpryiemstva: analiz naiavnykh vyznachen [Economic security of the enterprise: analysis of existing definitions] *Bulletin of the Poltava University of Econ. and Trade Visnyk Poltavskoho universytetu ekon. i torhivli.,* **69**: 90–95.

Liashenko, A.N. 2008. Vzaiemozalezhnist i vzaiemozalezhnist ekonomichnoi bezpeky i rozvytku pidpryiemstva [Mutual dependence and mutual dependence of economic security and development of the enterprise] *Bulletin of Donetsk State University of Management,* **45**: 162–171.

Lipych, L. and Skoruk, O. 2020. Providing financial and economic security of the enterprise in the conditions of development of the digital economy. *Econ. J. of Lesia Ukrainka Eastern European National University,* **3**(23): 106–113.

Liubokhynets, L., Rudnichenko, Ye., Dzhereliuk, I., Illiashenko, O., Kryvdyk, V. and Havlovska, N. 2020. Methodological foundations of flexible management and assessing the flexibility of an enterprise economic security system. *Int. J. of Scientific and Techno. Res.,* **9**(3): 4616–4621.

Maresova, P., Soukal, I., Svobodova, L., Hedvicakova, M., Javanmardi, Ehsan Selamat, A. and Krejcar, O. 2018. Consequences of Industry 4.0 in business and econ. *Econ.,* **6**(3): 1–14.

OECD, 2015. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264245471-en.

OECD, 2020. Chapter 7. Digital security https://www.oecd-ilibrary.org/sites/a5efc19a-en/index.html?itemId=/content/component/a5efc19a-en.

OECD, 2020. The Role of Public Policy and Regulation in Encouraging Clarity in Cyber Insurance Coverage, OECD, Paris, http://www.oecd.org/finance/insurance/The-Role-of-Public-Policy-and-Regulation-in-Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf.

OECD, 2021. The Digital Transformation of SMEs URL: https://www.oecd.org/industry/smes/PH-SME-Digitalisation-final.pdf.

OECD based on Eurostat, 2019. Digital Economy and Society Statistics, Comprehensive Database StatLink https://doi.org/10.1787/888934192357.

OECD based on Eurostat, 2019. Digital Economy and Society Statistics, Comprehensive Database. StatLink https://doi.org/10.1787/888934192376.

Parmacli, D.M. 2015. Effektivnost' zemlepol'zovaniya i ehkonomicheskaya bezopasnost' sel'skohozyajstvennyh predpriyatij [Land-use efficiency and economic security of enterprises], Chapter 6, in D. M. Parmacli, *et al.* Jeffektivnost' zemlepol'zovanija: teorija, metodika, praktika: monografija. Gos. un-t, Nauch.-issled. centr "Progress". Komrat: B. I. (in Russian).

Rausand, M. 2011. Risk assessment: theory, methods, and applications. Hoboken: John Wiley & Sons, Inc., Publication. http://dx.doi.org/10.1002/9781118281116.

Real, J.C., Leal, A. and Roldán, J.L. 2006. Information technology as a determinant of organizational learning and technological distinctive competencies. *Industrial Marketing Management*, **35**: 505–521.

Roztocki, N., Soja, P. and Weistroffer, H.R. 2019. The role of information and communication technologies in socioeconomic development: Towards a multi-dimensional framework. *Information Techno. for Dev.*, **25**(2): 171–183.

Scholz, T. 2017. Uberworked and Underpaid: How Workers Are Disrupting the Digital Economy Economy, Polity Press, Cambridge, UK.

Shutyak, Y., Danylenko, O. and Van Caillie, D. 2014. Conceptualization of economic security of the enterprise: a literature review, in 3rd REDETE Conference "Econ. Development and Entrepreneurship in Transition Economies", 10th April 2014, Banja Luka, Bosnia and Herzegovina, pp. 145–152.

Stankic, R., Jovanovic Gavrilovic, B. and Soldic Aleksic, J. 2018. Information and communication technologies in education as a stimulus to economic development. *Econ. Horizons*, **20**(1): 59–71.

Strelcova, S., Rehak, D. and Johnson, D. 2015. Influence of critical infrastructure on enterprise economic security, *Communications*, **1**: 105–110.

Suglobov, A.E. Hmelev, S.A. and Orlova, E.A. 2013. Jekonomicheskaja bezopasnost' predprijatija [The economic security of enterprise]. Moskva: Juniti – Dana (in Russian).

The Digital Economy and Society Index (DESI) (2021) URL: https://digital-strategy.ec.europa.eu/en/policies/desi.

Zečević, A. and Radović Stojanović, J. 2017. The Use of Information and Communication Technologies in Enterprises in Serbia. *Ekonomika preduzeća*, **45**(5–6): 393–403.

Zečević, A. and Radović Stojanović, J. 2018. The Use of Information and Communication Technologies in Enterprises in the Region: Level Achieved and Further Development. *In:* S. Drezgić, S. Živković and M. Tomljanović (Eds.). Economics of Digital Transformation (pp. 177–194). Rijeka, Croatia: University of Rijeka, Faculty of Economics and Business in Rijeka.

Zigunova, A., Shevkunov, N., Logvinova, I., Kislov, I. and Shevchenko, V. 2020. Ensuring economic security of the enterprise in anti-crisis conditions E3S Web of Conferences, **157**: 04030.