https://doi.org/10.33271/nvngu/2023-4/150

T. Kapeliushna[*1],
orcid.org/0000-0001-7490-6751,
A. Goloborodko[1],
orcid.org/0000-0001-5416-0526,
S. Nesterenko[2],
orcid.org/0000-0001-9090-3470,
I. Bezhenar[3],
orcid.org/0000-0002-4584-9062,
B. Matviichuk[4],
orcid.org/0009-0005-7030-9876

1 – State University of Information and Communication Technology, Kyiv, Ukraine
2 – Open International University of Human Development "Ukraine", Kyiv, Ukraine
3 – National Scientific Centre "Institute of Agrarian Economics", Kyiv, Ukraine
4 – Interregional Academy of Personnel Management, Kyiv, Ukraine
* Corresponding author e-mail: e-skr@ukr.net

ANALYSIS OF DIGITALIZATION CHANGES AND THEIR IMPACT ON ENTERPRISE SECURITY MANAGEMENT UNDER UNCERTAINTY

Purpose. To analyze the changes caused by the acceleration of digitalization under conditions of uncertainty and note their impact on enterprise security management in this environment.

Methodology. The methodological basis for the study was the theoretical provisions of enterprise security; legal regulations governing security and information protection, scientific works by domestic and foreign scholars on the issues of enterprise security management. The methods of analysis, synthesis, deduction, generalization and cognition were used in the study on the issue.

Findings. The conditions of functioning of enterprises are analyzed, in particular, the security of enterprises is considered in conditions of uncertainty caused by the martial law imposed in Ukraine and the acceleration of digitalization of business processes as a result of the emergence of new challenges.

Originality. A number of events are traced that preceded the increased interest in electronic services and active investment by enterprises related to e-commerce; artificial intelligence, big data; technology. The basis is investigated for the emergence of new challenges and threats associated with the active use of the Internet, applied solutions, servers, big data, data processing methods, the use of third-party software, i.e. the risks of violating the integrity, reliability, and confidentiality of information. The trends in measuring enterprise security are analyzed and the factors that strengthen the role of protecting information assets of enterprises and organizations are identified. It is proposed to pay more attention to ensuring the security of enterprises, taking into account not only physical but also invisible intrusions, such as: threats to information, the information field of enterprise functioning through a consistent response to cyber incidents/cyber-attacks by providing cybersecurity actors with protective stages: preparation, detection and analysis, deterrence, elimination, recovery, analysis of the efficiency of measures to respond to cyber incidents/cyber attacks.

Practical value. The analysis carried out proves the relevance of the issues of enterprise security, the formation of changes in views on enterprise security in accordance with current trends and uncertain conditions. The findings of the study can be taken into account and practically implemented in the formation of the enterprise security policy, regardless of the field of activity.

Keywords: *enterprise security, conditions of uncertainty, information threats, cyber security, digitalization of business processes*

Introduction. The key issue to be solved today is security in all spheres and branches of activity of economic entities, at all levels – from local to global. The current changes caused by the informatization of society, digitalization, processing of large volumes of data, the use of artificial intelligence, the emergence of the 5G mobile communication standard (in the near future, the 6G standard), the Internet of Things, and the growing demand for cloud services require a careful study on the current conditions and functioning peculiarities. Digital business access to new digital services requires rethinking approaches to security management while finding ways to ensure soft adaptation to the uncertain conditions caused by war in the country. The purpose is to outline the security and protection of the virtual infrastructure, in which the majority of businesses, educational institutions, and the state (providing digital services) currently operate, taking into account today's external challenges, primarily in the conditions of remote work and digitalization of business processes. That is, digital business, society, and the state need to detail the security of remote access in the post-quarantine period and military actions, which cause a number of challenges and strengthen and accelerate digitalization processes at all levels.

Literature review. In the uncertain conditions of functioning and challenges of modernity, the issue of adaptation of enterprises to transformational changes caused by digitalization, which is the result of a change in the technological structure and external security threats at the national level, is studied. Domestic and foreign scientists have devoted their work to digitalization issues: N. V. Proskurnina, N. A. Tyukhtenko, T. I. Oleshko, V. I. Kyfyak, H. Zhosan, N. Kyrychenko, T. Soest, O. V. Oliinyk, D. I. Shestakova, M. Rachinger, R. Rauter, C. Muller, W. Vorraber, E. Schirgi, E. Calderon-Monge, D. Ribeiro-Soriano. Fundamental studies on security, security management, approaches to enterprise security management were conducted by scientists: Ye. Ovcharenko, N. Zayed, et al., S. Levytska, et al., A. Sumets, et al.

The digital space of today's society and business produces risks associated with the violation of the integrity, reliability, and confidentiality of information, which is a valuable resource. The information possessed by the enterprise serves as the basis for decision-making, company management and the selection of directions for further development. All enterprise resources must be protected; information resources and technological solutions for their processing are no exception.

Therefore, issues of digitalization, adaptation to transformational changes occurring as a result of digitalization of society and business structures, the state and, in parallel with this, issues of security are relevant and are actively researched. Thus, N. V. Proskurnina noted that a quick response to changes, a proactive search for new ideas and a high readiness for digitization are the triggers for the successful transformation of the business model of retail enterprises in the conditions of the digital revolution. Innovation, digital intelligence and personalization are defined as the main competencies of a retail enterprise, which must be adequately used in order to win the competition [1].

The author N. A. Tyukhtenko found that the level of digitalization, maintenance and security of information and com-

munication technologies at the studied enterprises of the southern region of the country is unsatisfactory, since in the process of organizing and coordinating production processes there is almost no involvement of specialists in the field of information and communication technologies, LAN networks (Local Area Network) are not used. In addition, maintenance of the infrastructure of information and communication technologies, support and development of software and ensuring the protection of confidential information is carried out only with the involvement of specialists from external companies [2], which significantly increases the risks of data theft.

The work by T. I. Oleshko, in which not only the relevance of digitalization of business processes is noted, but also at the same time security issues are emphasized as a priority direction of enterprise development, is worthy of attention. It is noted that airlines use Internet of Things technologies for physical infrastructure elements, special navigation programs that analyze information from sensors about the location of objects are being developed. Taking into account the importance of the development of the transport sector, as one of the critically important for the state, the scientist emphasized that the primary direction in the digitalization of the aviation industry is the formation of security through an individual (personalized) approach to each individual passenger and the work of the entire airline staff that is organized and adjusted at the highest level [3].

Kyfyak V.I. in her work noted that digitalization complicates risk management due to the blurring in time and space of risk boundaries, which become uncertain and difficult to predict in the digital environment, and emphasizes the need for institutional support for risk management and digital tools as a necessary component of business models in modern conditions [4].

Scientist H. Zhosan proposes an approach with sequential disclosure of stages (levels) in the process of digital transformation of business and its formation as a digital ecosystem. The logic of this process includes five stages: updating digital initiatives; the beginning of digitization; adoption of digital reality; self-regulation and multivariate foresight; open digital ecosystem.

In business, there should be an adjustment to information processing using advanced digital capabilities, technologies, which will lead to an improvement in the organization of work and an adjustment of the business culture of enterprises in accordance with innovative technological changes and opportunities that arise when implementing digital technologies in the work [5].

Soest T. outlined the main trends of the restaurant business, in particular: to ensure a flexible and immediate response to the fast-moving and changing market environment, it is suggested to use cloud technologies; to optimize costs (calculation of the cost of meals, permissible product waste, etc.) – it is possible to conduct an analysis of the cost part in the request mode for the use and implementation of elements of "artificial intelligence"; customer service in uncertain conditions is made possible through the formation of online orders. In addition, the issue of environmental sustainability, the desire of consumers to be informed about the origin of products from which dishes are prepared, as well as their supply network, is also mentioned. The transparency of this chain is ensured by using the Internet of Things technology [6].

Oliinyk O. V. and Shestakova D. I. note that in business, digital transformation helps to optimize and increase the accuracy of individual business processes and suggests the transfer of various areas of activity of economic entities to electronic platforms (management, sale of products and their payment, interaction with customers, etc.), which ensures the growth of the competitiveness of this business with the active use of digital solutions [7].

Rachinger M., et al. explored the differences and similarities between how digitalization affects a company's value creation, its offering and customer engagement, as well as how businesses cope with the challenges, arising in connection with the growth of digitalization. According to their results, digitalization is generally considered an important factor, and its position in the value network determines the available opportunities for business model innovation (BMI) under the influence of digitalization. Organizational capabilities and employee competencies in security issues have been identified as future challenges that companies will face [8].

Calderon-Monge E. and Ribeiro-Soriano D. point out that the digital transformation affects the activities of companies in a number of industries and causes such consequences as fundamental upheavals in business models at the industry level and transformations of business practices at the organizational level. Scientists consider digital technologies to be one of the main drivers of economic growth and sustainable development in the modern business world [9]. Machine learning technologies help the extractive sector find important information and patterns that cannot be easily seen by industry engineers, and can automatically identify risks in the oil pipelines and infrastructure, resources and energy industries.

In the scientific work Ye. Ovcharenko considers a security management system with the possibility of using an intelligent agent, which builds the sequence of task execution, deadlines for their execution, determines the relationships and relations between similar agents with further cooperation, the possibility of activation, neutralization, as well as the use of the memory of other agents to form a safe environment [10].

In the works by N. Zayed, et al. it is rightly determined that for effective and permanent risk management at the enterprise, the need to obtain a sufficient amount of information, both from outside and inside the enterprise, must be ensured [11].

In the scientific work by S. Levytska, et al. on security and its management at enterprises, it is noted that there is no universal decision-making mechanism and one of the solutions is seen to be the consideration of the specifics of the business sector and the search for technological solutions and the improvement of management approaches in extreme situations, which are relevant at the present time [12].

Sumets A., et al. paid attention to the formation of the enterprise security management system, in particular, the scientist systematized the factors influencing the security of enterprises with proposals for solving the problems of economic security for telecommunications enterprises [13].

However, despite the number of publications and the significant contribution of scientists on the issues of ensuring and managing security, taking into account its role and importance in the modern computerized environment, there remain open questions that are closely related to the consequences of digitalization processes, as well as the threats that arise for enterprises that function in the online environment.

Unsolved aspects of the problem. Scientific developments in the formation of the security of the functioning of enterprises are valid and well-argued; however, further research is needed on the issue of digitalization changes, their impact on security management in conditions of uncertainty and acceleration of digitalization of business processes.

The purpose of the article is to analyze the changes caused by the acceleration of the digitization process in conditions of uncertainty, as well as to note their impact on the security management of enterprises under these conditions.

Methods. The methodological basis for the study was the theoretical and practical provisions of the security of the functioning of enterprises, statistical data of international organizations, normative legal acts regulating the issue of security and information protection, scientific works of domestic and foreign scientists devoted to the issues of enterprise security management. The methods of analysis, synthesis, deduction, generalization and cognition were used in the process of researching the given question.

Results. In recent years, the question of the rapid transition of enterprises to the online environment of functioning

due to the informatization of society, innovative discoveries, and the active use of Internet services, software, and applications has arisen.

The urgency of reformatting the functioning of enterprises in the digital plane has increased: the spread of the pandemic around the world, quarantine restrictions, and about a year ago uncertainty was added due to a full-scale invasion and the introduction of martial law in Ukraine. The dynamism of economic development and digitization stimulate monitoring of challenges and threats, the list of which is growing due to the emergence of new uncertainties against the background of war.

The study on digitalization issues is attracting more and more attention from scientists all over the world, as it is relevant at the global level, regardless of the operating conditions, because currently we exist in the times of transition to Industry 4.0, which involves the use of such technologies as: digital ecosystems, the Internet of things, big data analytics (Data Driven Decision), digital platforms and systems for managing business processes. This was preceded by the rapid development of information and communication technologies, the automation of production processes with their subsequent robotization; in addition, the role of the IT sector and the expansion of the range of services provided by telecommunications enterprises should not be forgotten.

Currently, the opportunities of the sectors vary, in particular, the following ones are currently developing: automotive industry, processing of agricultural products, furniture, metalworking and IT. According to Ukraineinvest, the telecommunications sector has a positive trend towards growth in the volume of computer services provided, the increase in the export of which in 2021 compared to the volume of 2020 was 26.3 %. Computer, telecommunication and information services exported abroad were worth 3,856.6 million US dollars. It is important that in the structure of exported services, telecommunications (computer services were mostly provided to residents of other countries) make up almost a third – 29.3 %.

It should be noted that in the conditions of martial law, as evidenced by the data of the Ministry and the Committee for Digital Transformation of Ukraine, the IT sector continues to develop steadily, the volumes of services provided are growing. During the first six months of 2022, which were extremely difficult for Ukraine, the increase in exported computer services amounted to 3.74 billion dollars (an increase compared to 2021 by 23 %).

Currently, the IT sector plays an important role in all areas of security, including society for the prevention of dangers that threaten future generations (ensuring sustainable development). Structural transformation, sustainable, inclusive and digital direction of development, which are taking place in the world, require changes in views on the functioning of enterprises in accordance with these trends.

The challenges caused by the pandemic, the complication of geopolitical relations, and wars, are increasing. In conditions of uncertainty, innovative technological solutions are widely used, enterprises are rethinking how to protect themselves from systemic risks, which is seen to be solved through the integration of digital capabilities into the work of enterprises.

Digital tools, the latest technologies should be used in order to increase the management efficiency of the enterprise, to fully use the latest digital opportunities and an expanded range of IT services. That is why the IT sector continues to demonstrate resilience in today's difficult conditions. During the period of the first half of 2022, 65 % of telecommunications enterprises were profitable, and 13 % of them increased their revenues by 25–30 % compared to the previous period [14].

Enterprises that are considered to be actively using technology and innovation are attracting more and more attention. In 2013, investor Eileen Lee coined the new term "unicorn" to refer to technological or innovative companies valued at more than $1 billion [15]. When analyzing the number of "unicorn" companies among European countries in 2022, the largest number of them is noted in Great Britain – 41, Germany – 25, France – 21 (Fig. 1) [16].

After analyzing the industries in which the aforementioned technological or innovative companies operate, it was found out that the largest number of them are in the field of IT, media, and telecommunications (Fig. 2). In addition, each subsequent group of "unicorns" by industry includes enterprises related to the use of the Internet and digitalization: e-commerce; artificial intelligence, big data; technologies and beauty [17].

The main Internet companies in terms of revenue in 2020–2022 are: Amazon.com; Apple; Google; Meta; Netflix; PayPal; eBay; Alibaba; Baidu; Tencent (Fig. 3).

During the last three years, among companies operating in the online sphere, the top three in terms of revenue have remained stable: Amazon (the manufacturing company is the largest on the market among e-commerce platforms) with revenue of 513.98 billion US dollars in 2022; "Apple" (the world's largest company by revenue in the field of information technologies, which is a manufacturer of personal computer equipment and software) with revenues of 394.3 billion US dollars; Google (supports and develops a number of Internet services and products) with revenues of 279.8 billion US dollars.

During the analyzed period, the leadership (The 100 Most Valuable Global Brands 2022) is held by the online retail company Amazon, which confidently occupies a leading position in terms of the volume of revenues and their stable growth. The Google company provides income primarily through Internet advertising, and the Apple company, which for the tenth year in a row is in the top ten in the annual ranking of the best global brands according to Interbrand, profits from the sale of the i-Phone, the use of which provides a number of advantages in the digital world through its own microservices offered by the company.

It should be emphasized that in the spring of this year, the technological giant Apple together with the financial Goldman Sachs Bank USA presented a financial product – a deposit account. A new service that will compete not with physical traditional banks, but with online banks using the digital wallet of the tech giant, is emerging.

The advantage of this service, among others, is the strengthening of the protection of financial resources, since access by third parties to the NFC chip (the technology that allows paying at the cash register of a store with one touch) is eliminated. Thus, we can conclude that the company is trying to integrate more deeply into the digital existence of users, offering a control panel for financial transactions that will be carried out by consumers.

Analyzing companies that are promising for capital investments, it is outlined that most of them are related to telecommunications, conducting trade through the Internet, process-

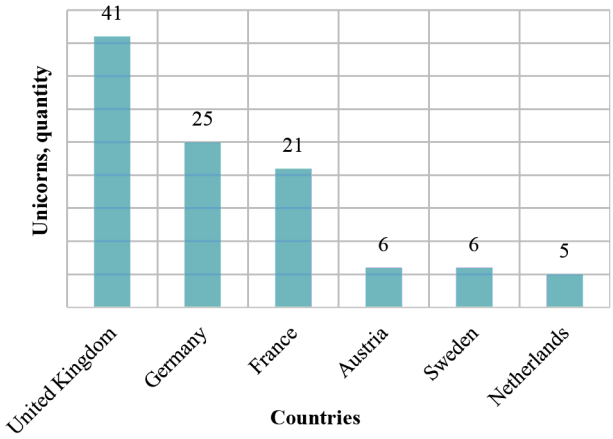

Fig. 1. Ranking of countries by the number of "unicorn" companies in 2022

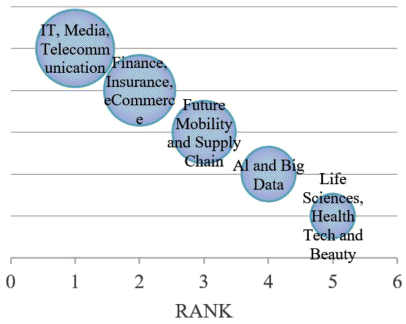

Fig. 2. Unicorn companies by the number and valuation of assets in 2022 (grouped by fields of activity)

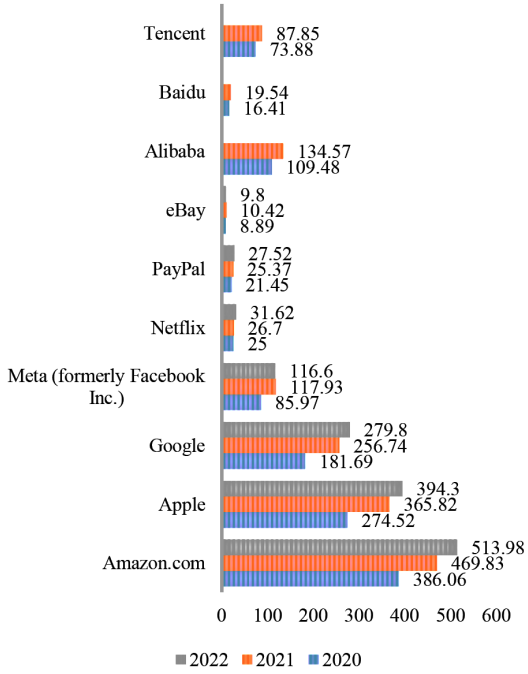

Fig. 3. Ranking of Internet companies by revenue volume during 2020–2022, billion USD

ing big data, that is, with activities in the sphere of IT and the global network. That is why information technologies, media and telecommunications are the first in the vertical in terms of the number of "unicorns" and the amount of investment. The explanation for such increased interest in electronic services, IT technologies and investment in these areas is a series of preceding events:

- internet availability, annual constant growth of the number of users of the global network;
- the combination of material and virtual into cyber-physical complexes that form a digital system in today's conditions, caused by the emergence of the Internet of Things, which enabled the exchange of information between people and devices;
- a pandemic that spread around the world and contributed to the transition of medicine, education, and business into the digital space, since the provision of educational and public services, conducting business operations, and trade were carried out using technologies, means of communication, and software;
- geopolitical tension and increased interest in high-tech developments in the field of defense.

In the period from 2021 to 2022, the share of Internet users in the countries of the European Union increased from 80.4 to 84 %, i. e. by 3.6 % (Fig. 4).

A steady upward trend has been observed over the past ten years, with an increase of 24.5 % since 2013 (from 59.5 % in

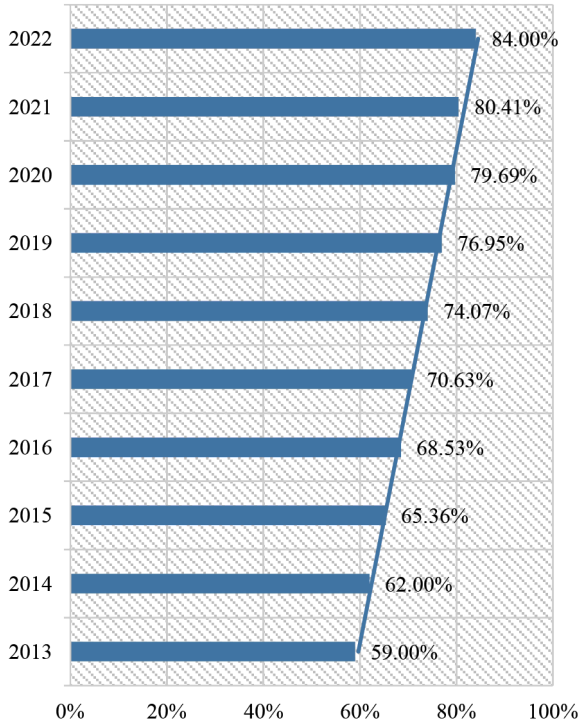

Fig. 4. Growth of daily Internet users during 2013–2022

2013 to 84 % in 2022). The explanation for this is the discovery in the fields of informatics, biotechnology, microelectronics, and satellite communications. By around 2015, a fifth wave of technological settlement is believed to have taken shape, when companies began to interact remotely from each other, building transnational networks and using electronic means of communication for their rapid communication.

Today's trends – the development of the digital plane, the integration of digital tools into the organization, allow business structures to remain competitive, increase the productivity of their activities, improve efficiency and resistance to the current uncertain conditions, which were previously caused by the pandemic, and now continue due to the armed aggression of the neighboring country against Ukraine.

Complicated operating conditions, external threats combined with new technological changes resulting from the fourth technological revolution and the fifth technological order, the latest trends in smart business with the use of artificial intelligence, GPT chat, special software, have led to intelligent and digitalized ways of doing business

In turn, these conditions serve as a basis for the emergence of new challenges and threats, which are associated with the active use of the Internet, applied solutions, servers, big data, data processing methods, the use of third-party software, i.e. risks of violation of the integrity, reliability, confidentiality of information.

While analyzing the results of research on security issues presented by the WEF (World Economic Forum), it was found that 14.5 % of respondents consider cyber security violations to be a critical threat to society in the next 2–5 years [18].

Information threats and their solution will be a priority in the next few years in terms of security and its provision in a dynamic digital environment, which today privileges and leads to transformational changes in the business environment. Often, businesses choose to source software from third parties, which creates technical dependency, which, in turn, creates the basis for the theft of information assets.

Currently, cyber theft is no less a threat than physically causing a security breach, as it leads to distortion of information, compromise of the company, theft of intellectual property, developments, data leakage, as a result of which the company bears economic losses.

Analyzing statistical data on the distribution of cyber-attacks in 2022 by industry [19, 20], their activity is observed in the world, production companies account for a quarter of the total number (Fig. 5).

Cyber fraudsters have a strong interest in information leaks in the banking and insurance sectors (19 % of cyber-attacks in 2022), as information leaks and data theft in financial institutions allow attackers to obtain the necessary information to steal financial assets. The vast majority of payments are currently made cashless, using web applications, so the security of their operation is one of the main priorities in the data protection policy.

Such operating conditions of business entities as: business automation, remote work and learning, artificial intelligence and technological changes lead to shifts in delineating flexible and smart, innovative ways of doing business and processing large volumes of data, integration of digital technologies in business organizations, which will generate new threats – cyber threats.

As it is mentioned above, threats of information leakage and violation of its integrity, cyber theft of confidential data, personal information, government data and data from business information systems pose a serious threat to the stable and effective functioning of enterprises, organizations, and the state.

It can be confidently stated that the search for overcoming risks that could potentially arise as a result of the realization of challenges and threats to information security is a priority in the digital field of society and business entities, which is confirmed by data on the number of malicious attacks in the world, starting from 2015 (Table).

The frequency of attacks reached peak values in 2018 – 10.5 billion attacks were registered in the world. The main targets used to harm organizations with malware were email, websites for phishing attacks. The attacks led to financial losses for organizations and companies, so public and private sector enterprises were forced to react to this situation in order to prevent potential negative consequences.

Starting from 2020, the number of attacks in the world decreased significantly, and in 2022 it amounted to 5.5 billion attacks. One of the reasons for the positive dynamics in the direction of decreasing attacks is the growth of spending on cyber security and information security insurance.

According to Next Move Strategy Consulting [21], the revenue of the cyber security market in 2022 was $289.32 billion (Fig. 6.)

Further growth of the market is predicted, so in 2030, revenues are expected to increase to 657.02 billion dollars (the growth rate compared to 2022 will be 227.1 %).

Security management due to the transition of organizations, enterprises to the digital space and the daily active use of the global network in everyday life, the increase in online stores, e-commerce platforms during the pandemic, blockchain, cloud computing, the use of artificial intelligence and

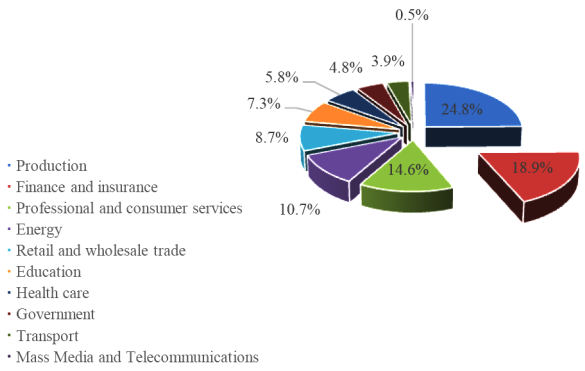

Fig. 5. Distribution of cyber-attacks in 2022 by industry (world)

Table

Frequency of malware attacks in the world during 2015–2022, billion attacks

Years	2015	2016	2017	2018	2019	2020	2021	2022
Number of attacks, billion	8.2	7.9	8.6	10.5	9.9	5.6	5.4	5.5

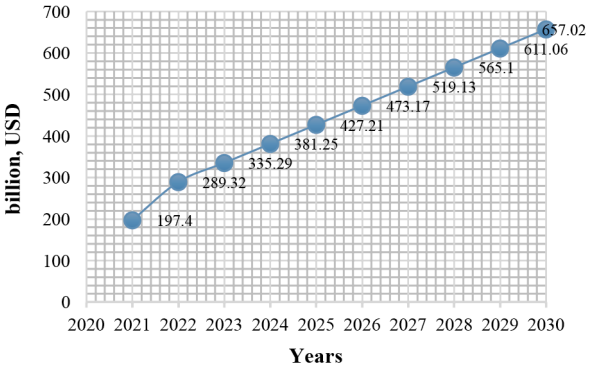

Fig. 6. Revenue from the cyber security market from 2021 to 2030, billion USD (predicted values)

the availability of GPT chat in Ukraine from the fall 2022, underline the urgency of data protection and security enhancements.

In addition, fraud has recently become widespread due to criminals gaining control over company equipment and devices in order to demand monetary rewards in exchange for returning management and control over the devices to the owners.

Among such programs is ransomware, which allows attackers to gain access to devices with files, to encrypt them, which leads to the shutdown of the enterprise. Further restoration of the company's activities is possible only if the perpetrators decrypt the files after payment of funds in their favor.

Clients and the business environment must be sure of the safety of their financial, property, and intellectual investments. That is why companies strive to protect information and financial assets, preserve their reputation in the information space, guarantee the safety of operation, which contributes to the growth of the cyber security market. The focus on protecting data, information, and the information field of enterprise activity will be maintained in the coming years, as evidenced by the analysis of enterprise security trends in the near future in the context of digitalization of society and uncertain conditions.

Conclusions. So, taking into account the analyzed trends in the dimension of enterprise security, we can single out factors that strengthen the role of protecting information assets of enterprises and organizations, which can be attributed to:

- use of cloud platforms for data storage (protection of cloud infrastructure using technologies and policies to protect information);
- digitization and informatization of society;
- digitization of services (mainly state);
- increase in the number of company personnel working remotely;
- lack of understanding of information security threats and data protection measures on the part of employees;
- big data processing;
- distribution of Internet of Things;
- the possibility of using the GPT chat widely since last November;
- modernization of corporate technologies and reduced understanding of the threats that arise with their appearance;

- use of information technology supply chains by organizations;

- fast-changing threats and the growth of their types in contrast to the lack of security service personnel.

The role and importance of security is increasingly strengthened due to informatization, digitalization and conditions of uncertainty of the functioning of enterprises during martial law. The conducted research emphasizes the importance of responding to incidents that threaten information, as it becomes a special resource in today's conditions of digitization, remote work, processing of large data sets, use of cloud services and chain supply of information technology services.

In the Resolution of the Cabinet of Ministers of Ukraine [22], it is determined that: "response to cyber incidents/cyber-attacks is carried out by subjects of cyber security by taking cyber protection measures aimed at quick detection and protection against cyber incidents/cyber-attacks, proper information about them, prevention of negative consequences, their minimization and elimination, the correction of vulnerabilities, as well as the restoration of stability and reliability of the functioning of information, electronic communication, information and communication systems, technological systems and other objects of cyber protection".

This is exactly what the protection of enterprises should be: to include not only physical intrusions, but also invisible threats to information, the information field of the functioning of enterprises [23].

The response to threats that arise in the information space of enterprises and organizations must be thought out and formed in stages, starting with the preparation for responding to a cyber incident with the detection and analysis of its occurrence, then – the search for ways of containment or partial/complete elimination, after – the return of the enterprise to the mode of normal functioning and resumption of work, and at the end – diagnosing and conducting an analysis of the expediency of the measures taken to respond to cyber-threat incidents with their further assessment [24, 25].

Internet security, digital security, information security are gaining particular importance in today's uncertain conditions and at the same time digitalization processes, and its provision should be considered as a priority direction in the formation of the security of enterprises and organizations of any sphere, regardless of the organizational and legal form of business, since most of large and global companies have long been integrated into the Internet environment and continue their development in the global network, expanding the boundaries of their existence through the use of modern information communications.

The importance of guaranteeing the security of enterprises, reducing risks, protecting against unauthorized access to the information of business enterprises, eliminating the possibility of improper exploitation of systems, networks and technologies, protecting the information field is confirmed by the data obtained as a result of the study on the distribution of cyber-attacks by industry, the number of attacks carried out using malicious programs, misrepresentation and theft of confidential information due to intrusions into the work of business organizations over the past year. Security in all areas, including information, is a priority as businesses and organizations continue to function and personnel work remotely under the constant threat of air strikes and the stress of a digitized business environment during intense combat. In addition, further consideration of this issue will be necessary to ensure the safety of the functioning of enterprises in the post-war period.

References.

1. Proskurnina, N. (2020). Transformation of Business Models of Retail Enterprises in the Conditions of Digitalization. *Business Inform*, *10*(513), 384-391. https://doi.org/10.32983/2222-4459-2020-10-384-391.

2. Tyukhtenko, N. (2021). Transformation of business models of retailers in the context of digitalization. *Business Inform*, *20*(2), 33-45.

3. Oleshko, T. (2021). Digitalization of business processes in civil aviation. *Economy and State*, (4), 43-46. https://doi.org/10.32702/2306-6806.2021.4.43.

4. Kyfyak, V. (2022). Institutional support for business risk management in the context of digitalization. *Problems of innovation and investment development*, (28), 85-98. https://doi.org/10.33813/2224-1213.28.2022.8.

5. Zhosan, H., & Kyrychenko, N. (2022). Management of digitalization of business processes of the enterprise. *Economic synergy*, (4), 85-98. https://doi.org/10.539203/ES-2022-4-2.

6. Soest, T. (2023). Digital transformation in the food industry: Trends, examples, and benefits. *The Future of Commerce*. Retrieved from https://www.the-future-of-commerce.com/2021/04/23/digital-transformation-in-food-industry.

7. Oliinyk, O., Shestakova, A., & Yarmolyuk, D. (2023). Directions of the restaurant business digitalization. *Economics, management and administration*, (1(103)), 15-21. https://doi.org/10.26642/ema-2023-1(103)-15-21.

8. Rachinger, M., Rauter, R., Muller, C., Varraber, W., & Schirgi, E. (2019). Digitalization and its influence on business model innovation. *Journal of Manufacturing Technology Management, 30*(8), 1143-1160. https://doi.org/10.1108/JMTM-01-2018-0020.

9. Calderon-Monge, E., & Ribeiro-Soriano, D. (2023). The role of digitalization in business and management: a systematic literature review. *Review of Managerial Science*. https://doi.org/10.1007/s11846-023-00647-8.

10. Ovcharenko, Ye. (2014). Possibilities of Using Artificial Intelligence Tools in Harmonizing Goals in the System of Economic Security of an Enterprise. *Business Inform*, (12), 345-350.

11. Zayed, N. M., Edeh, F. O., Darwish, S., Islam, K. M. A., Kryshtal, H., Nitsenko, V., & Stanislavyk, O. (2022). Human resource skill adjustment in service sector: Predicting dynamic capability in post COVID-19 work environment. *Journal of Risk and Financial Management*, *15*(9). https://doi.org/10.3390/jrfm15090402.

12. Levytska, S., Pershko, L., Akimova, L., Akimov, O., Havrilenko, K., & Kucherovskii, O. (2022). A risk-oriented approach in the system of internal auditing of the subjects of financial monitoring. *International Journal of Applied Economics, Finance and Accounting*, *14*(2), 194-206. https://doi.org/10.33094/ijaefa.v14i2.715.

13. Sumets, A., Tyrkalo, Y., Popovych, N., Poliakova, J., & Krupin, V. (2022). Modeling of the Environmental Risk Management System of Agroholdings Considering the Sustainable Development Values. *Agricultural and Resource Economics*, *8*(4), 244-265. https://doi.org/10.51599/are.2022.08.04.11.

14. *JRC Big Data Analytics Platform* (2022). Retrieved from https://jeodpp.jrc.ec.europa.eu/ftp/jrc-opendata/RESILIENCE-DASHBOARDS/Spring2022Update/Dashboard_SpringUpdate_20220523.pdf.

15. Aileen Lee, C. (2013). *Welcome To The Unicorn Club: Learning From Billion-Dollar Startups*.

16. *The 2022 European Unicorn & Soonicorn Report - European Tech Startups*. European Soonicorn Unicorn Report 2022. Retrieved from https://europeanunicornmap.com.

17. Buchholz, K. (2022). *Infographic: Global Unicorn Herd Now Counts 1,000+ Companies*. Statista Infographics. Retrieved from https://www.statista.com/chart/27266/unicorns-by-country-world-map.

18. World Economic Forum (2022). *"The Global Risks Report 2022"* (*17th* ed.). Retrieved from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf (World Economic Forum).

19. Petrosyan, A. (2023). *Global distribution of cyber attacks in top industries 2022. Statista*. Retrieved from https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide.

20. *Number of malware attacks per year 2022 Statista* (2023). Retrieved from https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide.

21. Cyber security market (2022). Next Move Strategy Consulting. (2022). *NMSC. Cyber Security Market Analysis Report. 2022–2030*. Retrieved from https://www.nextmsc.com/report/cyber-security-market.

22. Verkhovna Rada of Ukraine (2023). *Some issues of response by cybersecurity entities to various types of events in cyberspace, Resolution of the Cabinet of Ministers of Ukraine No. 299*. Retrieved from https://zakon.rada.gov.ua/laws/show/299-2023-п#Text.

23. Bondarenko, S., Liganenko, I., Kalaman, O., & Niekrasova, L. (2018). Comparison of methods for determining the competitiveness of enterprises to determine market strategy. *International Journal of Civil Engineering and Technology, 9*(13), 890-898.

24. Kryshtanovych, M., Akimova, L., Akimov, O., Kubiniy, N., & Marhitich, V. (2021). Modeling the process of forming the safety po-

tential of engineering enterprises. *International Journal of Safety and Security Engineering, 11*(3), 223-230. https://doi.org/10.18280/ijsse.110302.
25. Hubanova, T., Shchokin, R., Hubanov, O., Antonov, V., Slobodianiuk, P., & Podolyaka, S. (2021). Information technologies in improving crime prevention mechanisms in the border regions of southern Ukraine. *Journal of Information Technology Management, 13*, 75-90. https://doi.org/10.22059/JITM.2021.80738.

Аналіз цифровізаційних змін та їх вплив на управління безпекою підприємств в умовах невизначеності

Т. В. Капелюшна[*1], *А. Ю. Голобородько*[1], *С. С. Нестеренко*[2], *І. М. Беженар*[3], *Б. О. Матвійчук*[4]
1 – Державний університет інформаційно-комунікаційних технологій, м. Київ, Україна
2 – Відкритий міжнародний університет розвитку людини «Україна», м. Київ, Україна
3 – Національний науковий центр «Інститут аграрної економіки», м. Київ, Україна
4 – Міжрегіональна Академія управління персоналом, м. Київ, Україна
[*] Автор-кореспондент e-mail: e-skr@ukr.net

Мета. Проаналізувати зміни, що викликані пришвидшенням процесу цифровізації в умовах невизначеності, а також відзначити їх вплив на управління безпекою підприємств за даних умов.

Методика. Методологічною основою для дослідження слугували: теоретичні положення безпеки функціонування підприємств; нормативно-правові акти, що регулюють питання безпеки й захисту інформації; наукові праці вітчизняних і закордонних учених, що присвячені проблематиці управління безпекою підприємства. Під час дослідження поставленого питання були використані методи аналізу, синтезу, дедукції, узагальнень і пізнання.

Результати. Проаналізовані умови функціонування підприємств, зокрема, розглянута безпека підприємств унаслідок появи нових викликів і загроз в умовах невизначеності, спричиненої впровадженням воєнного стану в Україні та прискоренням діджиталізації бізнес-процесів.

Наукова новизна. Відслідкована низка подій, що передували посиленому інтересу до електронних послуг і активному інвестуванню підприємств, пов'язаних із: е-комерцією; штучним інтелектом, великими даними; технологіями. Досліджене підґрунтя до появи нових викликів і загроз, що пов'язані з активним використанням мережі Інтернет, прикладних рішень, серверів, великих даних, способів обробки даних, використанням стороннього програмного забезпечення, тобто ризиків порушення цілісності, достовірності, конфіденційності інформації. Проаналізовані тенденції у вимірі безпеки підприємств, а також виокремлені фактори, що посилюють роль захисту інформаційних активів підприємств і організацій. Запропоновано більше уваги приділяти гарантуванню безпеки підприємств, ураховуючи не лише фізичні, але й невидимі вторгнення, такі як: загрози інформації, інформаційному полю функціонування підприємств за допомогою послідовного реагування на кіберінциденти/кібератаки через забезпечення суб'єктами кібербезпеки захисних етапів – підготовка, виявлення та аналіз, стримування, усунення, відновлення, аналіз ефективності заходів із реагування на кіберінциденти/кібератаки.

Практична значимість. Проведений аналіз доводить актуальність питань безпеки функціонування підприємств, формування змін у поглядах щодо безпеки підприємств у відповідності до сьогоднішніх тенденцій і невизначених умов. Отримані результати дослідження можуть прийматися до уваги та практично реалізовуватись при формуванні політики безпеки функціонування підприємств незалежно від сфери діяльності.

Ключові слова: *безпека підприємств, умови невизначеності, загроза інформації, кіберзахист, цифровізація бізнес-процесів*

The manuscript was submitted 13.02.23.