PROBLEMS OF CYBERSECURITY IN THE CONTEXT OF BECOMING AND DEVELOPMENT OF THE NEW ECONOMY

Hanna BEI

Vasyl' Stus Donetsk National University
600-richchya Str., 21, Vinnytsia, 21021, Ukraine, +380 (432) 50-89-48
e-mail: h.larycheva@donnu.edu.ua

Abstract

In the context of the formation and development of a new type of economy, the ability of organizations to accumulate competitive advantages while ensuring the security of economic activities without the threat of loss or misuse of digital data accumulated as a result of socio-economic interaction is becoming increasingly important. The article discusses the main trends and problems of cybersecurity in the conditions of a new type of economy, the impact of human and social factor on the formation of organizational and national cyber stability, the directions of digital security and cyber threats overcoming at the micro, meso and macro levels. Existing trends and tailbacks in the operation of cybersecurity systems have been identified, the impact of the personnel training level on the degree of cyber threats occurrence has been considered, as well as possible ways to overcome them in the context of global digitalization of business processes. As a result of the study, a close relationship has been established between policies to manage human resources potential, the degree of labour involvement, its competence and the risks of cyber threats, along with the speed of its spread. Directions of human potential of the organization activation are proposed in order to prevent the emergence of digital threats and reduce the degree of their negative impact.

Keywords: *Cybersecurity, Digitalization, High skilled, Human Capital, New Economy.*

JEL Classification: O33; J24

INTRODUCTION

The formation of a new type of economy in modern conditions is accompanied by complex and multi-stage processes of technological transformation which affect all spheres of social and economic development of society. The new or digital type of economy development is today associated with the wide spread of advanced technologies of production, robotics and automation, new mobile sources of data accumulation and widespread distribution of Internet communications, cloud computing, big data analytics, artificial intelligence [13; 16].

Digital technologies in the new economy rather than information technologies are aimed more at the internal components of effective economic activity [8]. Above all, intensive use of new technologies enhances the level of communications and interconnections, expanding the possibilities of unimpeded and effective interaction between various economic and social actors in a single digital space. This, on the one hand, leads to increasing their competitiveness, improving business processes, forming a new, flexible structure of cooperation, strengthening national and global cooperation. Research by the McKinsey Institute found that about 90% of management in the UK and US expect digital and information technology to significantly enhance strategic benefits for their business [5]. On the other hand, universal digitalization carries serious risks, as the subsequent data sets of misuse can result in significant reputational and economic losses, as well as loss of established competitive advantage.

Cybersecurity in most studies is seen as the cornerstone of the digital economy, which determines the degree of confidence digital information users have in various economic and social structures, as well as government regulation [2; 3]. Simultaneously such technologies as sensors,

mobile communication, cloud computing and big data become more and more integrated into the different industries, causing the need for reliable and stable system of safe storage and transfer of corporate data. The World Economic Forum mention a problem of cyber security among one of the most serious risks of further development when losses from the implemented cyber-attacks by 2021 can reach from $3 to $6 trillion by different estimates [18].

Ensuring the digital security of business means not only the need for a flexible system of government regulation that simultaneously controls the dissemination and use of personal and commercial data and does not limit the freedom to conduct business, still the development of a well-designed strategy for the safe creation, accumulation and processing of information at the micro level is important.

Recognition that with the further development of technology the number of cyber-attacks will only increase acquiring new and atypical forms, becoming more targeted and causing significant damage, company leaders should take cybersecurity as one of the most important issues, paying attention to any factors that can increase its cyber-sustainability.

Very often the human factor acts as an origin of cyberthreats when security breach is made through the slightest error in the code of the software or negligence in procession of data, the insufficient level of professionalism in interaction with the digital interface and also problems of social and psychological and behavioral character [17]. Prevention of similar threats belongs to the most significant difficulties of cybersecurity today, the same time not all CEOs of the companies understands that the solution of this problem through staff dismissal or toughening of control measures is not always the most correct.

Human and machine intelligence will be increasingly closely linked in the future, and the quality of this interaction will depend among other factors on the level of human resources development. Today organizations lack a highly professional workforce and are looking for ways to overcome this situation through corporate systems of personnel development, talent management, cooperation with higher education institutions, etc. [12]. Reason why the preventive formation of a labour force of the necessary quality and professionalism which is capable to cover quickly a wide range of technological and conceptual changes in the target sphere while preventing violations of the security of the internal corporate space is one of the most important tasks of the development of the new economy.

MATERIAL AND METHOD

Theoretical and practical research and results of modern scientists in the field of digital economy have allowed to deepen and expand understanding of the importance of cybersecurity in conditions of increasing technological development, To justify the prerequisites for the gradual transformation of the concept of cybersecurity towards cyber-sustainability and assess the importance of existing cybersecurity problems in the new economy, analytical and statistical materials of digital risk research institutes have been used. This has highlighted bottlenecks in the digital security system, including the importance of the human factor. In order to identify the relationship between the efficiency of the management system and the level of staff involvement and the degree of reliability of cyber threat prevention systems an analysis of internal documents of industrial enterprises was carried out.

RESULTS AND DISCUSSIONS

The concept of a new economy is increasingly used today by scientists as a definition of the economic sphere post-industrial period rapid development phenomena under the influence of digitalization and its distinctive technological changes. This implies the organic integration of the traditional economy properties with the new digital elements, the transition to a higher topological level, the priority of the service sector, the focus on improving the standard of living and the quality of education [1; 4]. Other authors refer to call the tendency to rapidly increase innovative potential and share of high-tech industries, intellectualization of human capital and turn it into the main resource of creating additional cost, strengthening globalization and integration processes as a main component of the new economy [9]. Summarizing the characteristics of the new economy it should be noted that its driving force and production resource are knowledge, and the use of new technologies repeatedly enhances the development opportunities, the products produced become less material, the character and structure of work takes an intellectual and innovative form, the geographical and national boundaries of interaction are erased, the dynamics of all processes are significantly accelerated.

In earlier studies [15] the new economy is often called the digital economy based on the widespread distribution of information and communication technologies; however, this definition of economy covers only a narrow part of all the transformations characteristic of the post-industrial period of economic development. The new economy causes significant changes in the construction of business models, market formation, properties of goods and services making it the object of research of many scientists, so the information and technological aspects in this sense are sidelined. At the same time, the digital aspect of its development is equally important, as it defines a new type of interaction between all economic and social agents, erases the boundaries of opportunities and shifts attention to three key components: the creation of new, unique digital products and devices for its use, the application of new digital models of interaction (cloud technologies, digital platforms, digital services), working with huge amounts of data.

Through the effective application of the opportunities offered by digitalization the new economy is seen as a driving force for economic growth, capable to lead very quickly to significant shifts in all spheres of life and overcome the lag in its quality. Such a jump could be most beneficial to developing countries, where the results would be much more visible than in the category of highly developed countries. On the other hand, the digital economy not only provides opportunities, but also poses threats, especially if digital skills and technology penetration are low enough. In addition, the transition period is accompanied by several negative phenomena, such as lack of resources, rising unemployment, institutional vulnerability, lack of opportunities, etc., as a result of which active growth is possible only in countries where a certain technological base already exists.

The most significant digitalization is for micro-level when targeted and strategically coordinated application of digital technologies, especially ready-to-use products, such as cloud computing, mobile technology, sensors, Internet of Things (IoT), big data, cognitive technologies (AI), augmented reality (AR), robotics, addictive manufacturing (3D printing), drones and others, can be easily integrated into existing business systems, involves changing the business architecture and all related processes, increases the speed of information exchange, moreover, is based on the quality of its accumulation, distribution and analysis, which determines the current and future competitiveness [8].

The use of digital technologies requires a high level of trust in transactions and at the same time the building of trust is constantly threatened by the increasing activity of cybercrime. Despite the fact that most part of CEOs around the world call technological renewal and digitalization the main priority of development, at the national level specialized programs to support digital transformations are actively

developed and implemented, the issue of ensuring the safety of economic activity remains a problem of the new economy and significantly affects the degree of its spread.

Cybersecurity is defined today as one of the five most significant risks of today 's world. On the one hand, the improvement and development of digital technologies provides an opportunity to accelerate the development of the business environment, promotes competitive advantage, strengthens communication and interaction with clients, allows to more accurately adjust the properties of the created product to their requirements, as well as allows to track and more quickly introduce innovations, provides a number of other important advantages. At the national level, digitalization helps to accelerate the performance of State bodies 'functions in the management and regulation of economic and social processes, facilitates citizens' access to public services and enhances their participation in decision-making and influence on local and regional development. At the same time, facilitating access to personal information, the digital nature of its transmission and processing, the shadow segment of the application of advanced technologies leads to an increased risk of further use of digital products and services, especially in conditions of economic and political instability of global scale.

Cybersecurity is defined today as one of the five most significant risks of today 's world. On the one hand, the improvement and development of digital technologies provides an opportunity to accelerate growth of the business environment, promotes competitive advantage, strengthens communication and interaction with clients, allows to adjust the properties of the created product to the consumer requirements more accurately, as well as permission to track and more quickly introduce innovations, provides a number of other important advantages. At the national level digitalization helps to accelerate the performance of government functions in the management and regulation of economic and social processes, facilitates citizens' access to public services and enhances civil participation in decision-making and influence on local and regional development.

Simultaneously, facilitating access to personal information, the digital nature of its transmission and processing, the shadow segment of the application of advanced technologies leads to an increased risk of further use of digital products and services, especially in conditions of economic and political instability of global scale.

Cyber security incidents can incite very negative impact on many levels (individual, institutional, organizational, corporate, national) and cause direct financial and other damages (data breach, downtime, inability to implement business processes, critical infrastructure instability, etc.) and have much more dangerous indirect effects (stolen identity, personal fraud, legal obligations, lost privacy, loss of reputation, bad public image, wellbeing decrease).

In the report of the World Economic Forum on the assessment of global world risks in terms of probability in 2019 data fraud and theft together with the problem of cyber-attacks are among the top five threats along with three environmental risks (extreme weather changes, global disasters, failure of climate-change ratification and adaptation) the last two years [18]. In addition, more than two thirds of respondents note also a high level of economic losses due to the spread of fake news and loss of privacy of private companies and governments caused by massive violations identified in 2018 in the security of Big Data storage, new hardware weaknesses, as well as potential exposure to cyber-attacks under uses of artificial intelligence. Cyber-attacks pose risks to critical infrastructure, prompting countries to strengthen their screening of cross-border partnerships on national security grounds. The largest number of cyber-attacks is in the health sector (28%), the financial and banking sector (20%), consumption (12%) (Fig.1).

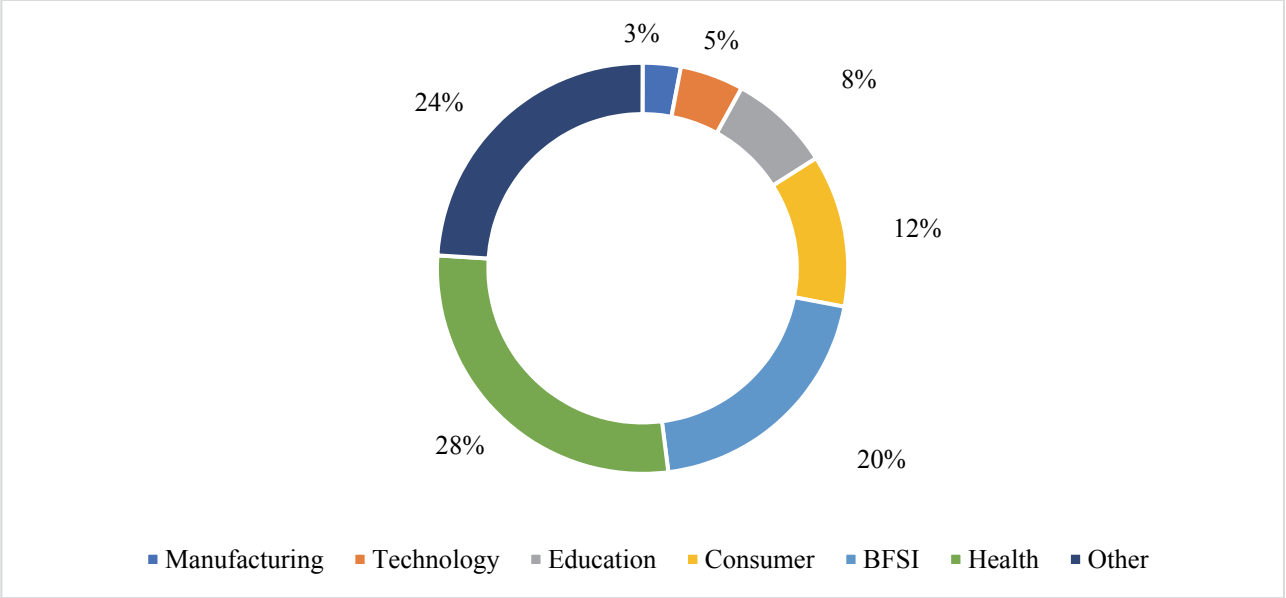

Fig. 1 – *Distribution of cyber attacks by economic sector in 2018*
Source: State of Cybersecurity Report 2019 [14]

At the same time the largest number of threats came from activity of suspicious applications, fake social networks profiles, e-mail addresses, as well as violations of digital security rules by users, vulnerability of chat bots and messengers, direct shadow attacks [14].

The risk of a cyber-attack ranks second among the top 10 global risks of doing business alongside the possibility of a fiscal and labour market crisis not only in US, Canada, the UK and Germany, but also edged out all other risks in France and Italy to occupy the top spot for the first time [7]. Business owners estimate the possibility of being hacked at 74% and the total economic damage from cyber-attacks will reach more than $3 trillion annually, and it is impossible to guarantee 100% protection of critical technological infrastructure (such as Supply Chain and Transport, Electricity, Aviation, Travel and Tourism, IoT, Nuclear Security, Banking and Capital Markets etc.) despite the intensive development of digital technologies .

In 2018, 61 companies in the European Union announced the detection of at least one cyber-attack on their business compared to 45 statements last year and the number of these statements is increasing (Fig. 2). Research shows that SMBs are most susceptible to attacks, which are 77% targeted.

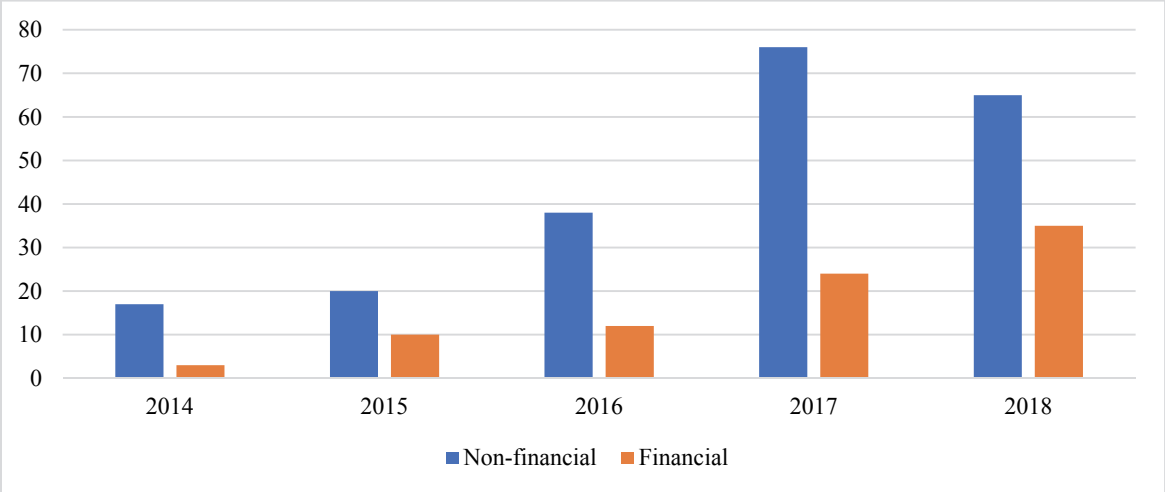

Fig. 2 – *Level of cyber-attacks on the financial and non-financial sector in the European Union, %*
Source: Hybrid and cybersecurity threats and the European Union's financial system [7]

Germany 's industrial union estimates that German companies suffered damage in more than €43 billion from data espionage and sabotage during 2016-2017, and 7 out of 10 companies are targeted for cyber-attack each year. All at once, the UK Government notes a slight decrease in the number of companies attacked (up to 32% compared to 43% in the previous year) [7].

In the private sector, over the next five years companies risk losing an estimated US$5.2 trillion in value creation opportunities from the digital economy to cybersecurity attacks. The largest number of financial losses is in High Tech (753$ billion loses), Life Sciences ($642 billion), Automotive ($505 billion), Consumer Goods & Services ($385 billion), Banking ($347 billion), Health ($347 billion), Retail ($340 billion), Insurance ($305 billion) etc. [11].

Due to the higher risk and increasing number of attacks cybersecurity is gradually evolving into the notion of cyber-resilience or sustainability [10], from the goal of providing protection mainly by preventive measures (Information security) to detect the attack, predict its consequences, develop countermeasures as early as possible, minimize the consequences (Cybersecurity), further to readiness for permanent damage due to cyber threats and the fastest possible restoration of the specified level of functioning of critical infrastructure and business processes (Cyber-sustainability) (Fig. 3).

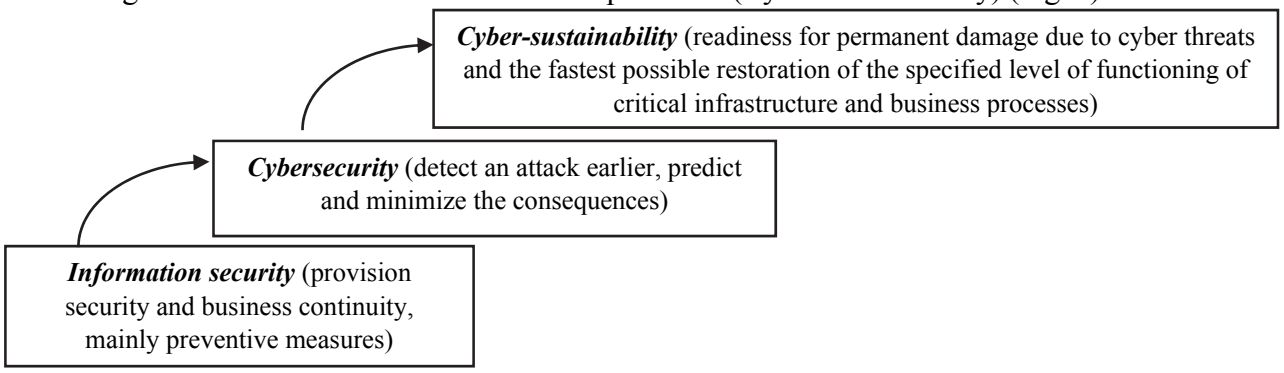

Fig. 3 – *Evolution from the organization 's cybersecurity to its cyber-sustainability*
Source: Developed by the author based on the [2; 3; 10]

Today organizations should be able to work in an environment where businesses need to be prepared to be deliberately damaged by the constant impact of cyber threats. In addition, cyberthreats influence people 's psychology and behavior, affect their lives and can undermine all efforts to achieve economic and social sustainability for individuals, businesses, countries and the world.

Digital trends are changing rapidly and despite various limitations in most countries of the world are quickly learning the possibilities of artificial intelligence (Deep learning, Machine Learning, Smart robots), augmented reality (4D-print, AR, VR), digital platforms (5G, Digital Twin, Blockchain, IoT, Quantum Computing). The most commonly used digital technologies in 2019 include: Digital Twin, Conversational User Interfaces, Digital Ethics, Chatbots, Cloud Office, Cloud Access Security Brokers, Virtual Assistants, Machine Learning, IoT Platform, Augmented Reality [6]. Each of these areas and technologies poses its own multitude threats up to the threat of harm to health, as they involve the use of big data, the new challenges in the field of cybersecurity which include the impossibility of existing protections to ensure the security of data of this size; labour-intensive verification of the authenticity of data sources and data integrity control; increasing criticality of Big Data access control processes; increasing risks of data unavailability and loss.

Malicious cyber-attacks and lax cybersecurity protocols again led to massive breaches of personal information starting in 2018 and continues. Single penetration can damage a huge number of users, and personal data can be resold or distributed many times, as in the case of the incident in India, when stolen data was sold at Rs. 500 in 10 minutes or when leak at a state-owned utility company allowed anyone to

download names and ID numbers, and more than 150 million users of the MyFitnessPal application and around 50 million Facebook users have learned of the misuse of their identity.

Cybervulnerability is characteristic not only to work of the software or applications, attacks on computer hardware rather than software when the perfect attack potentially could affect all processors of the Intel company released for the last 10 years gain distribution today. Besides, machine learning or artificial intelligence (AI) is becoming more sophisticated and prevalent, with growing potential to amplify existing risks or create new ones, particularly as the Internet of Things connects billions of devices [18]. Attackers have become more sophisticated, engineering targeted strikes resulting in a higher breach rate (notional records stolen per second increased from 43 to 232), And, to a greater extent, they are shifting to the most profitable areas, whose disruption threatens the global stability of the entire economic system.

Speaking about the change in the behavior of attackers, it should be noted that in recent years attacks have become more accurate, adjusted and allowed at one time to get the most profit and avoid punishment. So about 38% of attacks in 2018 were aimed at combining of Personally Identifiable Information (PII) and security credentials like passwords. On the one hand, it is caused by the improvement of technologies to overcome threats, the development of systems of response and prevention, on the other - the desire of attackers to remain focused on one sphere and less vulnerable to digital trace.

The nature of the attacks does not exclude use of already proved harmful technologies, such as trojans (57%), web penetration (22%), remote coding and controlling (15%). Along with it the level of the attacks on cryptocurrency mining servers and use of unreliable information for the purpose of discredit opponents' executives through social platforms grew up (fake profiles from Consumer & Retail sector, LinkedIn, Facebook, Twitter) [14].

The danger is also that without overcoming the problems of the existing technologies cyber-invulnerability developed countries and companies that are constantly investing in innovation are already having to form strategies for the introduction of new, only emerging technologies, such as [6]:

- Sentiment and Mobility (more accurate understanding and modeling of the world around us through the combination of sensory technologies and artificial intelligence: 3D-sensing cameras, AR cloud, light-cargo delivery drones, flying autonomous vehicles and autonomous driving);
- Augmented Human (enable creation of cognitive and physical improvements as an integral part of the human body: biochips, personification, augmented intelligence, emotion AI, immersive workspaces and biotech);
- Postclassical Compute and Comms (next generations of computing, communication and integration technologies with entirely new architectures: 5G, next-generation memory, LEO systems and nanoscale 3D printing);
- Digital Ecosystems (interdependent group of actors (enterprises, people and things) sharing digital platforms to achieve a mutually beneficial purpose: DigitalOps, knowledge graphs, synthetic data, decentralized web and decentralized autonomous organizations);
- Advanced AI and Analytics (the autonomous or semiautonomous examination of data or content using sophisticated techniques and tools, typically beyond those of traditional business intelligence (BI), include adaptive machine learning (ML), edge AI, edge analytics, explainable AI, AI platform as a service (PaaS), transfer learning, generative adversarial networks and graph analytics).

The vector of development of advanced technologies indicates the following changes in the field of cybersecurity:

– speed of emergence of new technologies increases, the landscape of threats extends with the increasing speed, and threats, as well as technologies, become more complicated;

– the number of the attacks (as well as their complexity) increases exponential;

– the amount of vulnerabilities does not decrease, and opposite, grows as to complication of technologies and development tools;

– the trend on detection and reaction instead of prevention and neutralization of cyberthreats leads to change of behavior of attacking, their adaptability to neutralization measures grows;

– cybersecurity skills and capabilities are the main concerns for organizations.

With further improvement technology of artificial intelligence will be capable not only to create much quicker the malicious software and to get into the unprotected systems, but also to generate harder and harder threats based on ability to distinguish human emotions, to answer them and to manipulate them.

The problem of technological dependence and empathy further increases the risk of cyber-vulnerability, as it affects the emotional and mental components of human behavior. The feeling of loneliness and depression can be enhanced by creating the illusion of community and "connect with others in a meaningful way," and in the case of a properly chosen manipulation mechanism lead to unpredictable behavior of individuals and groups. This is particularly important in the context of the co-laboratory interaction of people in the workplace, where the lack of a sense of unity, command spirit and importance of the labour contribution can cause serious economic and reputational losses. In addition, technological and societal change is linked to rapid transformations in the workplace and what happens at work has the potential to affect emotional and psychological well-being.

In order to reduce the risk of cyberthreats, public and private organizations work to create a single sustainability strategy and tactics, the first of which was the Australian Government 's "Critical Infrastructure Resilience Strategy" of 2010. Later, other organizations joined the issue: Big4 (PWC, EY), analytical agencies (Gartner), vendors (IBM, Symantec) and NIST, European Central Bank. Some organizations (EY1, Gartner, NIST2) focus on building a cyber-resilience cycle, while others suggest building and improving a cybersecurity risk management system (PWC3).

To increase resilience against hybrid and cyber-attacks against the financial system, the EU has taken a three-part approach: regulations and standards, testing and preparedness, governance. Attempts to promote cybersecurity, including for financial market infrastructures (FMIs), have led to several initiatives at all levels: globally, at EU level and at national level [7]. But despite a large list of approaches to cybersecurity, a unified methodology for measuring and assessing cyber stability has not been developed.

At the same time, it is worth noting the positive developments in the field of cybersecurity caused by consistent and systematic support of the concept of achieving cyber stability by senior management, the effective functioning of specialized structural units, the development of measures for comprehensive monitoring and detection of threats, timely response and recovery if they are implemented, continuous improvement of cybersecurity management system. This has led to a 17% increase in the level of positive sentiment among senior management about the reliability of their cybersecurity systems compared to 2013 (Fig. 4).

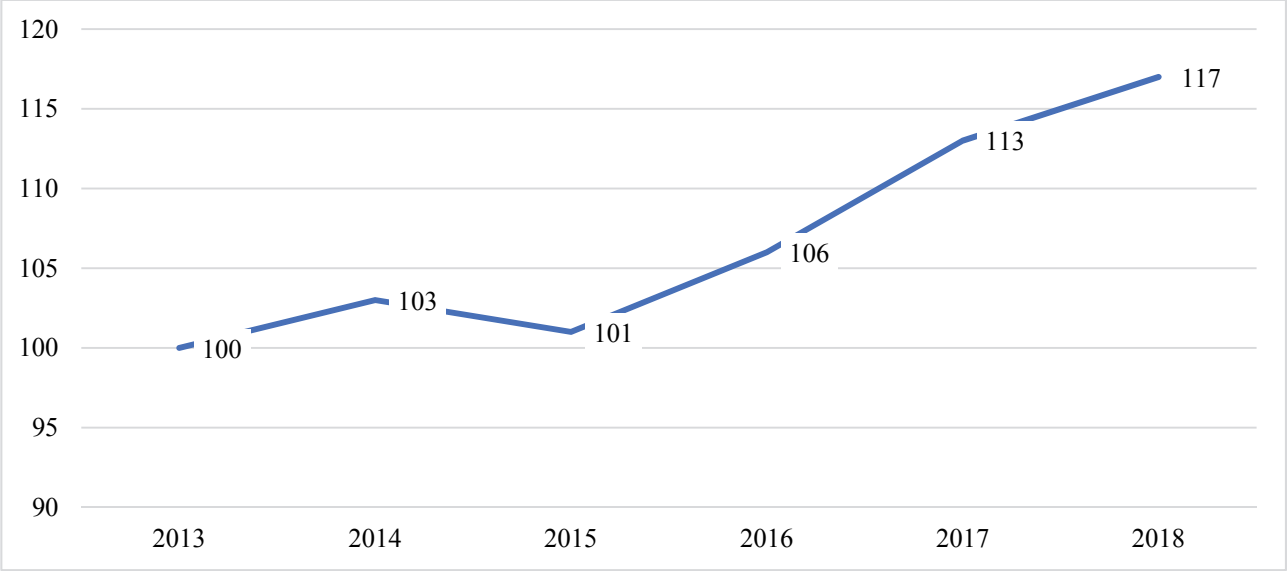

Fig. 4 - *CEO Sentiment Toward Cybersecurity, 2013-2018, %*
Source: Securing the digital economy. Reinventing the Internet for Trust [11]

Unfortunately, such trends are more common in developed countries, where the problems and threats of cybersecurity have long been understood, and innovative measures are being developed and implemented to prevent threats and reduce economic risks. In countries such as Ukraine and the less developed countries, the problem of cybercrime and cyberthreats is not seriously treated, economic risks are not assessed, and preventive measures are not developed or financed. Here the need for special training of personnel, creation of functional units responsible for cybersecurity issues (CISO), attention to cybersecurity issues and assessment of this issue in terms of risks and impact primarily on the business of the company come to the fore.

Qualitative work to prevent cyber threats is directly related to an effective system of human capital management. Whether the management system functions effectively, leaders can keep their employees motivated and focused on the result, how accurately the security relationship system is built, whether employees feel their involvement and responsibility for the quality of the work done, and they are ready to follow the established rules of digital behavior directly depends on the degree of cyber-sustainability of the company.

Too serious safety measures can cause staff psychological discomfort, which is only exacerbated by technological dependence, can lead to dissatisfaction with work, reduce their level of involvement, satisfaction with the quality of personal and working life. This vulnerability results in staff becoming more emotionally unstable, reducing productivity, more frequent conflicts, and thus more susceptible to targeted cyberattacks, fatal mistakes and the risk of cyberthreats. 72% of the cases of security violations in the world are related to lack of knowledge or human negligence, including in Ukraine, where the latest examples of cyber-attacks carried out (Petya/Nyetya, Ransomware, WannaCry) revealed serious gaps in the technical side of the issue, lack of effective process of tracking and response to detected attacks, established system of timely software update and backup.

The neglect personnel elementary rules of cyber security, lack of necessary basic skills and knowledge, the low level of the involvement of personnel, inefficient work of department of CISO or its absence, work with the unlicensed software, etc. appeared the greatest problem at the same time. Many employees had no action program on a case of detection and blocking of cyberthreat, were afraid to report on the incident to the top management or tried to overcome threat independently. Comparing among themselves results of internal monitoring of the industrial

enterprises affected by cyber-attacks in Ukraine, it should be noted that subordinates are more inclined to confer responsibility for cyber security on the manual (61.5%), but at the same time are informed on the level of own responsibility only on a third (29.8%), more than a half do not know how to behave in case of cyber-attack detection (52.0%) and do not feel that the digital security is a priority (43.5%), along with it, lack for knowledge of digital hygiene about 38.5%. Besides, the index of the involvement of personnel in these companies fluctuates within 0.35-0.69, and most successfully resisted to cyber-attacks of the company with the high level of basic and professional education of the employees where special attention is paid to the system of development and improvement of personnel.

CONCLUSION

On the basis of the above, the problem of cybersecurity in the new economy occupies a special place, as it is based on the widespread use of new digital technologies and devices that expand access to large amounts of information, accelerate and facilitate communications, change the architecture of doing business and building economic relations, at the same time, along with many positive effects it generates more and more new threats. The ability to gain access to vast amounts of personal and corporate data in one attack leads to an increase in the number of breach and changes in the behavior of attackers, who today focus on the most profitable sectors, such as finance and banking, health, consumption & retail, rely on already proven and completely new ways of malicious impact (from software to hardware).

Cybersecurity continues to be one of the leading issues in the list of global risks along with the problem of natural climate change due to the volume of economic losses as it also adds a socio-psychological factor caused by the increasing technological dependence of people and the ability of new technologies to recognize and manipulate human emotions. Accordingly, the acceleration of the development of new technologies now carries not only economic then also potentially dangerous risks to human life and health, including the exacerbation of states of depression, dissatisfaction and frustration.

This is particularly dangerous for the business where the coherence of all personnel depends on the overall result, and disregard for the problem of staff involvement and motivation in conditions of limited resources, inefficient policies of personnel management, lack of a system of training and development contributes to the strengthening of cyber-invulnerability. In addition, the study revealed that cybersecurity issues are being addressed mainly in those countries, regions, economic and business sectors whose organizational and national interests are constantly subject to cyber-attacks. Where attacks have not yet been recorded or are insignificant in number company executives do not even include cybersecurity costs in the annual budget.

On the basis of the assessment of the results of internal monitoring of industrial enterprises of Ukraine, which have suffered from large-scale cyber attacks of the last 2 years, the relationship between the level of staff involvement, efficiency of the management system, quality of internal corporate relations and the degree of cyber-invulnerability due to the fault of personnel has been revealed, which indicates the need to intensify scientific research in this direction.

REFERENCES

[1] Bell D, 1973, The coming of post-industrial society: A venture of social forecasting. New York: Basic Books, 616 p.

[2] Catherine Mulligan, 2017, Cybersecurity: cornerstone of the digital economy, available at: https://www.imperial.ac.uk/business-school/knowledge/technology/cybersecurity-cornerstone-of-the-digital-economy/
[3] Dmitry Markin, 2018, Cybersecurity – what it is and how to achieve it?, available at: https://bosfera.ru/bo/kiberustoychivost-chto-eto-takoe-i-kak-ee-dostich
[4] Forester T., 1987, High-Tech Society: The Story of the Information Technology Revolution, Oxford: Basil Blackwell, 311 p.
[5] Jacques Bughin, James Manyika, and Tanguy Catlin, 2019, Twenty-five years of digitization: Ten insights into how to play it right, McKinsey Global Institute, 12 p.
[6] Marcus Blosch, 2019, Hype Cycles: 5 Priorities Shape the Further Evolution of Digital Innovation: A Gartner Trend Insight Report, 11 p.
[7] Maria Demertzis and Guntram Wolf, 2019, Hybrid and cybersecurity threats and the European Union's financial system, 14 p.
[8] Mario Spremić, 2018, Cyber Security Challenges in Digital Economy. Proceedings of the World Congress on Engineering, Vol I, WCE 2018, July 4-6, 2018, London, U.K. 6 p.
[9] Martin R. Hilbert, 2001, From industrial economics to digital economics: an introduction to the transition. United Nations Publication, 133 p.
[10] Megan Stifel, 2018, Securing the Modern Economy: Transforming Cybersecurity Through Sustainability, 22 p.
[11] Omar Abbosh and Kelly Bissell, 2019, Securing the digital economy. Reinventing the Internet for Trust, 49 p.
[12] Regional dynamics of the global market: skills in demand and tomorrow's workforce. The Hays Global Skills Index 2017, 56 p.
[13] Schwab, K., 2015, The Fourth Industrial Revolution What It Means and How to Respond, Foreign Affairs, Science & Technology, December 12, available at: https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution
[14] State of Cybersecurity Report 2019, 2019, Wipro, 83 p.
[15] Tapscott D., 1995, The Digital Economy: Promise and Peril in the Age of Networked Intelligence, McGraw-Hill.
[16] Timothy J. Sturgeon, 2017, The 'New' Digital Economy and Development, UNCTAD Technical Notes on ICT for Development, 41 p.
[17] Serghei Ohrimenco and Grigori Borta, 2018, The shadow of digital economics, Year-book of D. A. Tsenov Academy of Economics, Svishtov, 61 p.
[18] World Economics Forum: Global Risk Report 2019, 2019, 14th Edition, 114 p.