sciendo

PRODUCTION ENGINEERING ARCHIVES 2023, 29(4), 379-392

PRODUCTION ENGINEERING ARCHIVES

ISSN 2353-5156 (print)
ISSN 2353-7779 (online)

Exist since 4th quarter 2013
Available online at https://pea-journal.eu

Company Cybersecurity System: Assessment, Risks and Expectations

Aleksandra Kuzior[1,2*], Hanna Yarovenko[3,4], Paulina Brożek[5], Natalia Sidelnyk[6], Anton Boyko[4], Tetyana Vasilyeva[7]

[1] Department of Applied Social Sciences, Faculty of Organization and Management, Silesian University of Technology; Roosevelt St., 26, PL 41-800 Zabrze, Poland; aleksandra.kuzior@polsl.pl
[2] Oleg Balatskyi Department of Management, Sumy State University; Rymskogo-Korsakova St., 2, 40007 Sumy, Ukraine
[3] Computer Science and Engineering Department, Carlos III University of Madrid; De la Universidad St., 30, 28911 Leganés, Madrid, Spain; hyaroven@inf.uc3m.es
[4] Economic Cybernetics Department, Sumy State University; Rymskogo-Korsakova St., 2, 40007 Sumy, Ukraine; h.yarovenko@biem.sumdu.edu.ua (HY); a.boiko@biem.sumdu.edu.ua (AB)
[5] JSofteris; 41-219 Sosnowiec, Poland; paulina.joanna.brozek@gmail.com
[6] Sumy Representative Office of the Insurance Company "VUSO"; Het′mana Pavla Skoropads′koho St., 4, 40000 Sumy, Ukraine; n.sidelnikh@gmail.com
[7] Department of Financial Technologies and Entrepreneurship, Sumy State University; Rymskogo-Korsakova St., 2, 40007 Sumy, Ukraine; tavasilyeva@biem.sumdu.edu.ua
*Correspondence: aleksandra.kuzior@polsl.pl

Article history
Received 01.08.2023
Accepted 15.09.2023
Available online 30.10.2023

Keywords
cybersecurity
cyber risk
cyber threat
Industry 4.0
Porter's method

Abstract
The consequences of Industry 4.0 have adverse side effects on cybercrime growth, which requires creating an effective cybersecurity system for companies. Therefore, this study aims to develop a composite indicator of company cybersecurity to assess its development needs. For this purpose, the authors modified Porter's method by constructing a superposition matrix based on the growth rates of cyber threats and risks, calculating their quantitative characteristics and a composite indicator. The computations are based on indicators for 2016-2022 characterizing cybersecurity vulnerabilities and the consequences of cyber threats: the share of companies experiencing one, six or more successful cyberattacks, considering the likely and very likely success of cyberattacks on them in the next 12 months, security threat and concern indices, the share of companies with a growing security budget affected by ransomware and experiencing a shortage of skilled IT security personnel, the cost of stolen or compromised credentials. As a result, cybersecurity needs increased significantly for 2020-2022, mainly due to digital transformation and the cyber threats growth after the COVID-19 pandemic. A comparative analysis of the proposed indicator with those characterizing the development of Industry 4.0 showed that the need for a reliable cybersecurity system is much more important than the active development of modern technologies. Spending on IT is also increasing, but not enough to meet the needs of cybersecurity development, except for the 2022 results. The proposed indicator is defined for companies worldwide, but its versatility allows the methodology to be applied to enterprises of various industries and sizes.

DOI: 10.30657/pea.2023.29.43

1. Introduction

Nowadays, society's development is accompanied by rapid scientific and technological progress, which many researchers have described as the Fourth Industrial Revolution or Industry 4.0. Its phenomenon has been substantiated by the German economist, founder of the World Economic Forum, Klaus Martin Schwab (Schwab, 2016). Industry 4.0 is associated with the development and implementation of cutting-edge technologies in various spheres of society's life, such as artificial intelligence, cloud and quantum computing, the Internet of Things, blockchains, augmented and virtual reality, nano- and neurotechnologies, autonomous robots, big data, and others. Most of them are already actively implemented and used

in companies and have shown their effectiveness in practice. External factors also adjust the business organisation and contribute to its transfer to cyberspace. For example, the global pandemic of COVID-19 became the impetus for active digital transformation of 46.3% of enterprises starting in 2021 (Michael, 2023).

On the one hand, these processes led to mass digitization and automation of economic relations. On the other hand, they became the cause of cybercrime appearance, identified as illegal actions committed with the help of computer technologies. Over the past fifty years, the cost of computers and their components has decreased significantly. For example, a computer chip with 2000 transistors cost $1000 in 1970, but today it can be purchased for $0.02 (Michael, 2023). This trend has resulted in the hacker device market offering tools for committing crimes starting at $1 (Rapp and Hackett, 2017). Business processes' digitization, automation, and technology availability to any user create favourable conditions for mass virus and DDoS attacks, cyberattacks on POS terminals, phishing, social engineering, control over the IT system, etc. It is not for nothing that the risk of cyber danger is one of the main ones for enterprises. According to the World Economic Forum (2023) for business, it is fourth after the cost-of-living crisis, natural disasters, extreme weather, and geoeconomic confrontation.

Experts estimated that the cost of global losses from cybercrime amounted to 8.44 trillion U.S. dollars in 2022, and their growth is predicted in 2027 to be 23.82 trillion U.S. dollars (Fleck, 2022). In most cases, companies suffer from cyberattacks, resulting in data leakage, stoppage of production processes, loss of customers, products, etc. The most targeted are enterprises in finance, information, professional, healthcare, manufacturing, public administration and education (Statista, 2023a). 91% of companies that are less than 50 million U.S. dollars lost less than 10 million U.S. dollars in 2018. At the same time, 28% of companies whose size exceeds one billion U.S. dollars received losses of more than 100 million U.S. dollars (Statista, 2022a). The most expensive attack was due to the spread of the ExPetr / NotPetya virus, resulting in companies losing 10 billion U.S. dollars (Greenberg, 2018). It is also possible to cite several examples of the consequences for companies due to massive cybercrimes directed against them. For example, the most prominent Indian power company, Tata Power Company Limited, was the victim of a cyberattack in October 2022, affecting its IT infrastructure (Lakshmanan, 2022). Due to hacking, Canadian meat company Maple Leaf Foods was forced to shut down its IT systems (Maple Leaf Foods, 2022). In February 2022, Toyota Motor Corporation suspended production on 28 lines at 14 plants, resulting in a 5% reduction in vehicle output, equivalent to a third of the global market (Hope, 2022).

The construction of any company's security system involves the development of a risk management concept, including cyber risks, which includes the analysis and assessment of dangers associated with its operation in the global cyber environment. Today, many companies are ready to spend significant money to implement leading technologies in their processes. Still, many of them are those, especially small ones, that do not increase the costs of IT budgets specifically for improving the cybersecurity system. It is because they do not have reliable data and appropriate techniques for assessing threats and the corresponding trends in companies' readiness to counter them. That is why the purpose of this study is to develop a composite indicator of company cybersecurity, which will allow to evaluate the need for the cybersecurity system development of enterprises based on the growth rate of cyber threats in the world and the level of cyber risks that they can cause. It will contribute to the formation of the readiness of enterprises to develop a cyber protection system to ensure the security of their activities.

2. Literature review

Issues related to the cybersecurity system of companies are relevant today, and their research is in the plane of various aspects - technical, organizational, economic, social, ethical, legal, etc. They also cover different subjects - the state, enterprises, and users. Moreover, the security capabilities of modern technologies are being investigated in various spheres of society's life, for example, health care (Pakhnenko and Pudło, 2023; Rekunenko et al., 2022), social services (Rahmanov et al., 2023), public administration (Pakhnenko and Kuan, 2023; Muradov, 2022). A bibliometric analysis of scientific publications devoted to cybersecurity issues in the context of Industry 4.0 was conducted for a more detailed understanding of research directions devoted to cybersecurity (*Appendix A, Figure 1*). Data from publications indexed in the Scopus database were selected for its implementation. As a result, 7 clusters were obtained with the help of the analytical package VOSviewer, which were formed based on associative rules established between the keywords of the articles.

The turquoise cluster (*Appendix A, Figure 1*) characterizes the direction of research on digital transformation, cloud computing, big data, distributed computer systems and robotics. Digital transformation affects the socioeconomic development of countries (Kuzior et al., 2019) and depends on the level of cybersecurity development (Kuzior et al., 2022). One of the critical factors of these transformational processes is digital literacy, which increases the efficiency of the personnel potential of enterprises (Tatli et al., 2023; Kobis, Karyy, 2021; Kuzmenko et al., 2021). Also, it can generate digital leadership in companies, which contributes to increasing the efficiency of many technological and security processes (Topcuoglu et al., 2023).

The lilac cluster (*Appendix A, Figure 1*) covers many publications on Internet of Things technologies, security, network security, machine learning, intrusion detection, e-learning and learning systems. Detection of vulnerabilities is an essential component of the formation of protection systems. Machine learning and intelligent data analysis methods effectively determine cyber threats' risks (Kuzmenko et al., 2020; Ievdokymov et al., 2020). In the conditions of emergencies that cyber threats can cause, analytical methods can be effective, allowing a quick express assessment under these conditions (Sergiienko et al., 2020). Convergent relationships exist between education, digitalization, and the economy, suggesting

the existence of sustainable interactions between them that contribute to the development of cyberspace, education, and the economy (Samusevych et al., 2021).

The orange cluster (*Appendix A, Figure 1*) is identified with the direction of computer crimes, intrusions detection, and decision-making. A promising method for detecting cybercrimes is digital forensics, which allows the identification of criminals by checking electronic data (Yarovenko and Rogkova, 2022). A technique of intellectual analysis can be applied to recognize different cybercrime, for example, committed based on social networks (Bozhenko et al., 2022). Vasilyeva et al. (2022) proposed a technique for determining phase portraits of victims of cybercrimes, which helps in early identification of signs of cyberthreats and timely response to them.

Research in the yellow cluster (*Appendix A, Figure 1*) concerns cyber-physical and embedded systems. In the framework of ensuring them, the most effective approach is based on identifying risks and dependencies between the cybernetic and physical components of such systems (Akbarzadeh and Katsikas, 2023). To strengthen their cyber protection, it is also possible to use digital doubles, which combine the digital and virtual worlds (Lampropoulos and Siakas, 2023; Skrynnyk, 2023).

The blue cluster (*Appendix A, Figure 1*) refers to a broad area of research dedicated to the issues of cybersecurity and Industry 4.0, which relate to artificial intelligence, blockchains and risk management. The industrial revolution provides many business development opportunities (Andrișan and Modreanu, 2022). But its challenges require strategic innovations in technologies such as blockchain, the Internet of Things, intelligent networks, cloud computing, and big data analytics (Kolosok et al., 2022; Wang et al., 2023, Kuzior et al., 2023, Kwilinski and Kuzior, 2020). Also, the transition to a new business model based on digitalization, cyberization, customization, etc., requires changes in human capital (Melnyk et al., 2021a). Transformational processes should also consider the risks associated with information technologies and the innovative development of enterprises (Skliar and Samoilikova, 2014).

The green cluster (*Appendix A, Figure 1*) characterizes the direction of cybersecurity regarding industrial control systems, critical infrastructure, malware and cyberattacks. Industrial control systems used to operate and control the critical infrastructure of enterprises are potential targets of cyber-attacks, so they need appropriate methods, such as machine learning, to predict cyber threats (Alqudhaibi et al., 2023). Cyber incidents can lead to failures of industrial control systems, so Masood et al. (2023) suggest using blockchain technologies as tools of the cyber defence system. When building security systems of industrial networks, it is necessary to consider several cybersecurity measures that will prevent the most destructive cyberattacks for them (Alrumaih and Alenazi, 2023).

Red cluster publications (*Appendix A, Figure 1*) are dedicated to research in the industrial revolution, smart manufacturing, augmented reality and data security. The paradigm of technology development is shifting towards intelligent production, which gives the right to call it Industry 5.0. Therefore, identifying cyber anomalies of such enterprises becomes acute, for which the XAI approach is proposed (Bac et al., 2023). There is also a problem with the integrity of big data of smart manufacturing, the solution of which can occur due to the application of the structure of blockchains (Juma et al., 2023). In addition, there are opportunities to implement augmented reality technologies to develop smart cities and intelligent production. Like other areas, they can become targets of cybercrimes, so they need security measures based on machine learning and artificial intelligence (Alzahrani and Alfouzan, 2022).

The bibliometric analysis demonstrated the existence of various research directions on the issue of company cybersecurity in the context of modern transformations caused by Industry 4.0. The obtained result indicates that this topic is multidisciplinary and requires a systematic approach and various methods and tools.

3. Experimental

This study aims to develop a Composite Indicator of Company Cybersecurity (we use the abbreviation CICCS further in the text), which will allow us to assess the need for progress in the cybersecurity system of enterprises, considering cyber threats and risks. For this purpose, a modified Porter's method was used as a non-linear form of convolution of relevant indicators based on a matrix approach. The following considerations justified the choice of this method: 1) the matrix approach will allow us to build an $m \times n$ matrix that will consider all possible combinations of input indicators for calculating the integral; 2) the strategic approach laid down in the idea of the Porter's method will allow us to determine strategic superpositions depending on the level of cyber risk and the rate of the cyber threat growth; 3) the possibility of its modification without reference to the basic methodology, that is, the formation of the author's matrix, providing it with quantitative characteristics and calculating the integral indicator based on the determinant of this matrix; 4) ease of implementation and interpretation of the obtained results.

The implementation of the method involved the formation of an input data array with ten indicators: 1) the share of organizations that experienced at least one successful cyberattack; 2) the share of organizations that have experienced six or more successful cyberattacks; 3) the share of respondents who believe that a successful cyberattack on their organization during the next 12 months will be "probable"; 4) the share of respondents who believe that a successful cyberattack on their organization during the next 12 months will be "very likely"; 5) the threat index, reflecting the general concern about cyberattacks; 6) security concern index; 7) the share of organizations with a growing security budget; 8) the share of organizations experiencing a shortage of qualified IT security personnel; 9) the share of organizations affected by ransomware; 10) the cost of stolen or compromised credentials. The source of indicators 1-9 statistics is the Cyberthreat Defense Report, based on a survey of representatives from 17 countries (CyberEdge Group, 2022). The source of statistical information for indicator 10 is the IBM report (IBM, 2022). The

survey respondents were more than 1,200 IT security professionals and more than 500 employees from companies in finance, government, telecommunications and technology, manufacturing, healthcare, education and retail from the USA, Great Britain, Germany, France, Australia, Brazil, Canada, China, Colombia, Italy, Japan, Mexico, Saudi Arabia, Singapore, South Africa, Spain, and Turkey. Thus, the selected indicators are based on the expert opinion of professionals in the cybersecurity field and adequately describe how companies understand the existing digital dangers and their readiness to spend financial resources to overcome cyber risks.

The first and second indicators (*Appendix B, Table 1, Line 1-2*) characterize the share of organizations that have experienced at least one cyberattack. If the first indicator describes a successful cyberattack on the organization, the second indicates the frequency of these attacks. The share of organizations that experienced at least one successful cyberattack grew by more than 4% on average between 2014 and 2022, and it exceeded 80% in the last three years. It means that there was a more active frequency of attacks. The average growth rate of the share of organizations that experienced six or more successful cyberattacks was 13.5%, and its value during 2020-2022 did not decrease below the level of 35%. It shows that the number of business entities whose digital systems are exposed to cyberattacks and the number of cyberattacks per company is increasing every year (Sidelnyk, 2023).

The third and fourth indicators (*Appendix B, Table 1, Line 3-4*) characterize the economic agents' expectations regarding the successful cyberattack. Since 2016, more than 60% of respondents believed that their company would likely be cyberattacked within the year. Since 2019, more than 20% of respondents were confident that a cyberattack on their company would be very successful and stop its activity for an indefinite period (Sidelnyk, 2023).

The fifth and sixth indicators (*Appendix B, Table 1, Line 5-6*) characterize the economic agents' concern regarding cyber threats. The threat index and the security concern index have been cyclical, with little swing since 2015. Thus, after a moderate decrease in the absolute value of the investigated indices in 2018-2019, their inevitable progressive growth is followed during the next year (by more than 7%) in 2021 and 2022. Based on the analysis results, we note that business entities are concerned with both the growing threat of cyberattacks and the inability of their digital security system to withstand the new challenges of digitalization (Sidelnyk, 2023).

The seventh and eighth indicators (*Appendix B, Table 1, Rows 7-8*) characterize the budgetary and personnel support for strengthening the cyber defence in response to cyber challenges. With the growing threat of cyberattacks, businesses and organizations increase their digital security budgets yearly. Thus, since 2018, more than 77% of business entities have increased their expenses for mechanisms to combat cyber risks. The indicator of the organizations' share experiencing a shortage of qualified IT security personnel confirms the active policy of business entities in the field of cybersecurity. Thus, during 2018-2022, the studied indicator consistently exceeded 80% (Sidelnyk, 2023).

The ninth and tenth indicators (*Appendix B, Table 1, Lines 9-10*) characterize the global consequences of cyber threats. Cyberattacks related to hijacking programs have also become common recently, affecting large and small businesses and affecting 70% of all surveyed respondents in 2022. Cyberattacks have also led to significant financial losses. During 2016-2022, economic entities lost an average of 3.9 million US dollars annually due to stolen or compromised credentials. Thus, it is fair to note that during 2014-2022, the activity of cyber threats to subjects has certainly increased, but despite the increase in the specific weight of the budget for digital security and efforts to expand the contingent of IT security specialists, the measures implemented are not enough to reduce the losses received and minimize the time of forced suspension of operations from cyber risks (Sidelnyk, 2023).

To form the CICCS, it was necessary to compare the selected indicators, as they are presented in three different units of measurement. For this purpose, the Savage method, formalized using formula (1), was used for destimulatory indicators.

$$p_{ij}^{norm} = \frac{\max\limits_{j}\{p_{ij}\} - p_{ij}}{\max\limits_{j}\{p_{ij}\} - \min\limits_{j}\{p_{ij}\}} \tag{1}$$

where p_{ij}^{norm} – normalized value of i-indicator in j-year, p_{ij} – the actual value of i-indicator in j-year, $i = 1 \div 9$, $j = 2016 \div 2022$.

The destimulatory indicators are indicators whose growth proves the deterioration of the cybersecurity situation. They included: p_1 – the share of organizations that experienced at least one successful cyberattack, p_2 – the share of organizations that experienced six or more successful cyberattacks, p_3 – the share of respondents who believe that a successful cyberattack on their organization will "probably" occur within the next 12 months, p_4 – the share of respondents who believe that a successful cyberattack on their organization during the next 12 months will be "very likely", p_5 – the threat index reflecting the general concern about cyberattacks, p_6 – the security concern index, p_7 – the share of organizations experiencing a shortage of qualified IT security personnel, p_8 – the proportion of organizations affected by ransomware, p_9 – the cost of stolen or compromised credentials.

In turn, it is proposed to use the natural normalization method (formula (2)) for the stimulator indicator (p_{10} – the share of organizations with a growing security budget). The growth of stimulator indicators shows the improvement and stabilization of the cybersecurity system.

$$p_{ij}^{norm} = \frac{p_{ij} - \min\limits_{j}\{p_{ij}\}}{\max\limits_{j}\{p_{ij}\} - \min\limits_{j}\{p_{ij}\}} \tag{2}$$

where p_{ij}^{norm} – normalized value of i-indicator in j-year, p_{ij} – the actual value of i-indicator in j-year, $i = p_{10}$, $j = 2016 \div 2022$.

2016-2022 was a period for calculations. It is due to the lack of statistical information for 2014-2017 for the share of organizations with a growing security budget, the share of organizations experiencing a shortage of qualified IT security personnel, the share of organizations affected by programs- by extortionists, the cost of stolen or compromised credentials.

The results obtained in the normalization process are summarized in *Table 2 of Appendix B.*

In the next step, the growth rates of each indicator's components of the CICCS composite indicator were calculated (*Appendix C, Table 3*). Based on the minimum, maximum and average values of the growth rates of these indicators, four ranges of cyber threat characteristics are established (Sidelnyk, 2023):

1) anticipatory growth of cyber threat: for 2016 – the growth rate is more than 16%, for 2017 – more than 19%, for 2018 – more than 3.5%, for 2019 – more than 7 .5%, for 2020 – more than 14%, for 2021 – more than 10%, for 2022 – more than 8%;

2) rapid growth of the cyber threat: for 2016 – the growth rate is within the range of 10%-16%, for 2017 – within the range of 9%-19%, for 2018 – within the range of 0%-3%, 5%, for 2019 – within the range of 4%-7.5%, for 2020 – within the range of 8%-14%, for 2021 – within the range of 6%-10%, for 2022 – within the range of 0%-8%;

3) moderate growth of the cyber threat: for 2016 – the growth rate is in the range of 8%-10%, for 2017 – in the range of 0%-9%, for 2018 – in the range of -2%-0 %, for 2019 – in the range of 0%-4%, for 2020 – in the range of 2%-8%, for 2021 – in the range of 0%-6%, for 2022 – in the range of -8%-0%;

4) reduction of the cyber threat: the growth rate is less than 8% for 2016, for 2017 – less than 0%, for 2018 – less than -2%, for 2019 – less than 0%, for 2020 – less than 2%, for 2021 – less than 0%, for 2022 – less than -8%.

Then, all indicators that are components of CICCS are proposed to be grouped depending on the level of this risk (based on the normalized values of these indicators) as follows (Sidelnyk, 2023):

- critical level of cyber risk (from 0.75 to 1.00);
- high level of cyber risk (from 0.50 to 0.75);
- average level of cyber risk (from 0.25 to 0.50);
- low level of cyber risk (from 0.00 to 0.25).

Due to the uneven distribution of indicators within the interval from 0 to 1, 2016 and 2021 became an exception (Sidelnyk, 2023):

- in 2016: 0.00-0.25 – low level of cyber risk; 0.25-0.60 – average level of cyber risk; 0.60-0.75 – high level of cyber risk; 0.75-1.00 – critical level of cyber risk;
- in 2021: 0.00-0.07 – low level of cyber risk; 0.07-0.15 – average level of cyber risk; 0.15-0.23 – high level of cyber risk; 0.23-0.30 - critical level of cyber risk.

Then, it is necessary to build a map of indicators that are components of CICCS in the form of a cross matrix. Depending on the calculated growth rate of the cyber threat and the cyber risk, those indicators that have common characteristics are highlighted and grouped.

In the cells of the superposition matrix of indicators ($b_{ij}, i = 1 \div 4, j = 1 \div 4$) that are components of CICCS, those are mentioned, which belong to this cell of the matrix according to the corresponding growth rate of the cyber threat and the level of cyber risk (*Appendix D, Table 4*).

The matrix B (formula (3)) is based on the construction of the superposition matrix of indicators that are components of CICCS (*Appendix D, Table 4*):

$$B = \begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix}. \tag{3}$$

Very often there is a situation when during formation of matrix B, its several elements b_{ij} take on zero values. In this case, the matrix elements are adjusted by adding a unit to them.

Based on matrix B, the quantitative value of the CICCS indicator is defined according to formula (4) by calculating the ratio of the matrix B determinant, as well as the square root of the sum of products of the elements forming the matrix:

$$CICCS = \frac{detB}{\sqrt{\begin{matrix} b_{11}b_{12}b_{13}b_{14} + b_{21}b_{22}b_{23}b_{24} + \\ +b_{31}b_{32}b_{33}b_{34} + b_{41}b_{42}b_{43}b_{44} + \\ +b_{11}b_{21}b_{31}b_{41} + b_{12}b_{22}b_{32}b_{42} + \\ +b_{13}b_{23}b_{33}b_{43} + b_{14}b_{24}b_{34}b_{44} \end{matrix}}} \tag{4}$$

where $CICCS$ – Composite Indicator of Company Cybersecurity, B – the superposition matrix of indicators that are components CICCS, $detB$ – determinant of the matrix B, $b_{ij}, i = 1 \div 4, j = 1 \div 4$ – the number of indicators that, according to the corresponding values of the growth rates of cyber threats and the level of cyber risk, refer to this cell of the matrix.

The numerator of formula (4) is calculated using the ratio (5):

$$detB = |B| = \sum_{(i_1, i_2, \dots, i_n)} (-1)^{\sigma(i_1, i_2, \dots, i_n)} b_{1_{i1}} b_{2_{i2}} \dots b_{n_{in}}, \tag{5}$$

where $\sigma(i_1, i_2, \dots, i_n)$ – the number of inversions in the permutation.

To simplify the mathematical expression, the denominator of the fraction is aggregated and transformed into formula (6):

$$CICCS = \frac{detB}{\sqrt{\begin{matrix} \prod_{j=1}^{4} b_{1j} + \prod_{j=1}^{4} b_{2j} + \prod_{j=1}^{4} b_{3j} + \prod_{j=1}^{4} b_{4j} + \\ + \prod_{j=1}^{4} b_{j1} + \prod_{j=1}^{4} b_{j2} + \prod_{j=1}^{4} b_{j3} + \prod_{j=1}^{4} b_{j4} \end{matrix}}} \tag{6}$$

Further transformations, namely the generalization of the sum of the components within the rows and columns of matrix B, will lead to obtaining the mathematical relationship (7):

$$CICCS = \frac{detB}{\sqrt{\sum_{i=1}^{4} \prod_{j=1}^{4} b_{ij} + \sum_{j=1}^{4} \prod_{i=1}^{4} b_{ij}}} \tag{7}$$

Considering the intermediate calculations given in formulas (4) - (7), the final version of the calculation of the composite indicator CICCS takes the form (8):

$$CICCS = \frac{\sum_{(i_1,i_2,\ldots,i_n)}(-1)^{\sigma(i_1,i_2,\ldots,i_n)} b_{1_{i_1}} b_{2_{i_2}} \ldots b_{n_{in}}}{\sqrt{\sum_{i=1}^{4}\prod_{j=1}^{4} b_{ij} + \sum_{j=1}^{4}\prod_{i=1}^{4} b_{ij}}}, \quad (8)$$

where |…| – absolute value of CICCS.

4. Results and discussion

In the process of implementing the proposed methodology, the adjusted superposition matrices were calculated to get the final value of the composite indicator (*Appendix E, Tables 5-11).* Their obtained values made it possible to determine the CICCS for each year for the research period (*Table 1*).

Table 1. CICCS calculated values for 2016-2022

Year	2016	2017	2018	2019	2020	2021	2022
CICCS	0.28	0.23	0.23	0.13	0.39	0.40	0.39

Source: calculated by authors based on Sidelnyk (2023)

In addition to the absolute CICCS values, the qualitative interpretation of the obtained results is also important. We will form three intervals with the help of root mean square deviation, namely:

1) CICCS from 0.34 to 0.50 – a high need to develop cybersecurity in the world. For companies, it means the need to make urgent management decisions regarding the introduction of new cyber protection technologies, measures to enhance the cyber literacy of employees, improvement of the cyber strategy, and revision of the IT budget in terms of increasing costs for cybersecurity;

2) CICCS from 0.17 to 0.33 – the average need to develop cybersecurity in the world. In this case, companies should form a proactive system for minimizing potential cyber risks through their cyber insurance, improve the cyber literacy of employees with the help of long-term training programs, evaluate the effectiveness of existing cybersecurity technologies and, under conditions of increased risks, formulate a plan for their renewal and strengthening;

3) CICCS from 0.00 to 0.16 – low need to develop for cybersecurity in the world. This option means that companies can focus on their core business processes and, at the same time, accumulate resources for the development of a robust system of protection against cyber risks in the following periods.

The need to develop cybersecurity in the world increased significantly in the last three years, reaching its maximum value in 2021 (the CICCS indicator in 2021 was 0.4 units). It is due to the conditions in which the world found itself because of the COVID-19 pandemic (Dluhopolskyi et al., 2023). They demanded quick decision-making at enterprises and reorientation of business processes in the cyber plane. The number of cases of cyber threats, which have turned into real cyber risks for companies, has increased. On the other hand, their willingness to deal with these risks and implement more powerful and effective security measures has also increased (Chen et al., 2023). During the previous three years (2016-2018), the need for cybersecurity development in the world was average since CICCS values ranged from 0.23 units up to 0.28 units. In 2019, the need for cybersecurity development in the world was low (the absolute value of the CICCS indicator was equal to 0.13 units). This value could be influenced by the fact that cyber threats in 2019 did not become critical risks for enterprises or they were better prepared for such situations.

The obtained CICCS indicator calculations are compared with the trends that describe the prospects of Industry 4.0, which are essential to developing the cybersecurity system of enterprises. One of these areas is artificial intelligence technologies, which are used to create intelligent machines and are implemented in engineering, robotics, medical systems, e-commerce, etc. Since artificial intelligence is based on the principles of human brain functioning, it can replace a person in solving various problems in the future. Therefore, their active implementation in the business sphere is currently underway. Figure 1 demonstrates the dynamics of cybersecurity development needs and revenues from artificial intelligence technologies. Rapid growth in implementing and using this technology exists for the global enterprise applications market. At the same time, their increase in 2023 by approximately 45% and in 2024 by about two times is predicted. Since it is necessary to develop cybersecurity, this trend in the behaviour of the artificial intelligence technologies market will also contribute to satisfying the demand for security systems in which they are implemented. Figure 1 shows that there will be a gap between the analysed indicators, which may indicate the prospects of artificial intelligence in the organization of enterprise security systems.

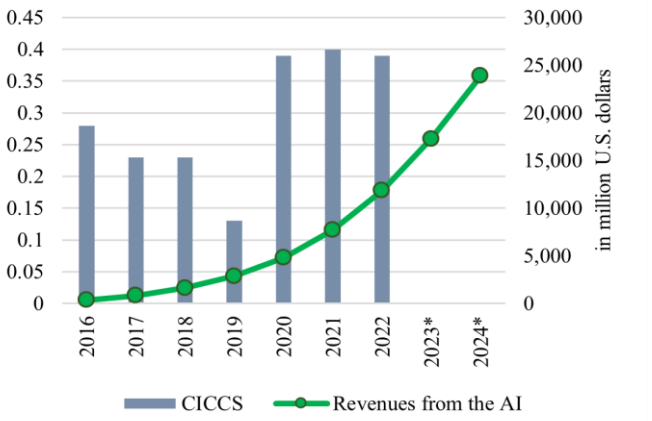

Fig. 1. Dynamics of the CICCS indicator and revenues from artificial intelligence for the enterprise applications global market for 2016-2024 (*2023 and 2024 contain forward estimates) (Statista, 2022b)

The next promising direction of Industry 4.0 is using industrial robots to perform various operations on industrial and technological lines. Their use helps increase labour productivity, and remote control capabilities increase company employees' safety levels. On the other hand, robotic systems will primarily suffer during cyberattacks on enterprise infrastructure. Therefore, they will need more effective cyber defence measures to reduce production downtime and costs to restore operational capacity due to a cyber threat. Figure 2 compares the need to develop the cybersecurity system and the volumes of installed industrial robots. Starting in 2020, one can observe their growth. Since the need for a robust cyber defence system

has increased over the past three years, compared to the demand for industrial jobs, they exceed the threats cyberattacks on industrial infrastructure can cause. Although by 2020, enterprises were also actively implementing this type of technology, the need for their cyber protection was much smaller.

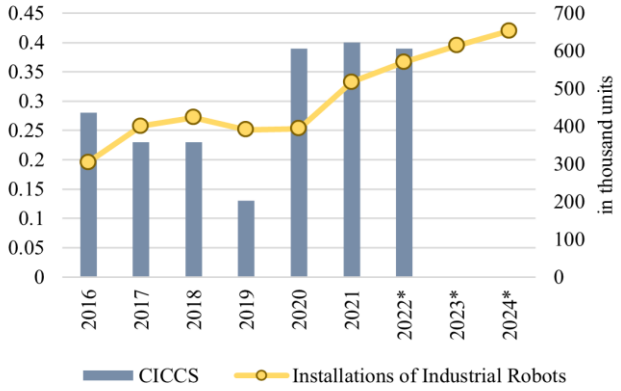

Fig. 2. Dynamics of the CICCS indicator and Installations of Industrial Robots for 2016-2024 (*2023 and 2024 contain forward estimates) (Rika, 2023)

Blockchain technologies have begun to be actively implemented in financial markets, but the scope of their application is significantly expanding (Kuzior and Sira, 2022) due to their security capabilities for organizing decentralized databases. Figure 3 presents the global blockchain technology market dynamics for 2016-2022, demonstrating an utterly positive development trend. Comparing the cybersecurity development needs with this technological direction; it requires more effort to organize the protection system. The level of cyber threats observed during the analysed period was quite serious for those companies that used blockchain. In 2022, this trend changed, which can only indicate the favourable conditions for the development of the cyber defence system concerning blockchain technologies.

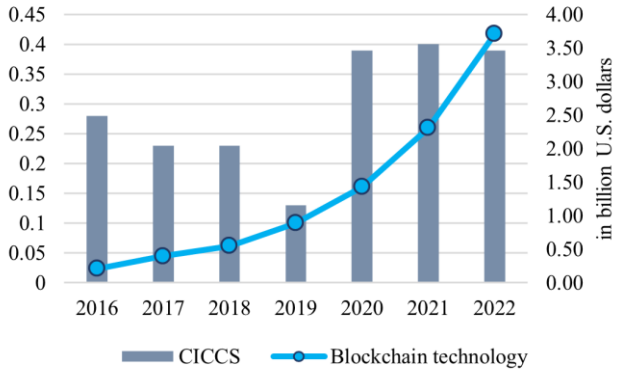

Fig. 3. Dynamics of the CICCS indicator and the global blockchain technology market for 2016-2022 (Statista, 2022c)

Internet of Things technologies have become part of the environment for automating industrial tasks. The main risks associated with their use are the risks of breach of confidentiality and information leakage, which require special cyber protection systems and protocols. Figure 4 demonstrates the positive dynamics of the global installed base of IoT-connected devices, including the projected growth of their volumes.

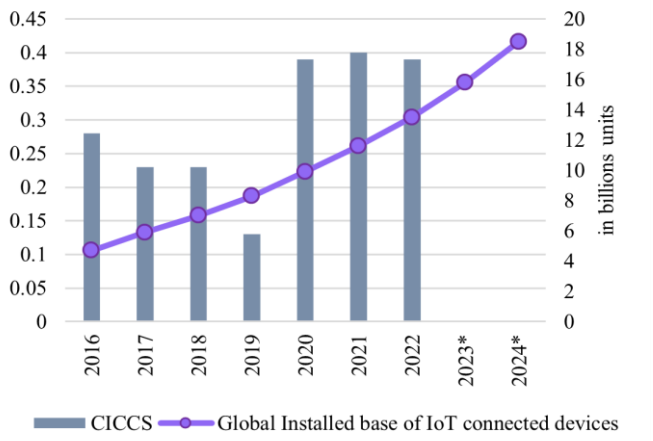

Fig. 4. Dynamics of the CICCS indicator and the Global Installed base of IoT connected devices for 2016-2024 (*2023 and 2024 contain forward estimates) (Reputiva, 2022)

Comparing this direction with the need for developing the cybersecurity system, one can see that they outweigh the volumes of established databases. Since they function through remote access, modern security measures do not 100% eliminate potential cyber risks, which requires additional cyber protection.

Figure 5 presents a comparison of the dynamics of IT costs and the need for the development of cyber defence. Until 2020, companies' IT budgets could cover the costs in this area, but starting from 2020, the need for cybersecurity has increased significantly, requiring new management approaches from enterprises. Many small businesses do not allocate additional funds for their cybersecurity because they believe the costs can be greater than the losses from cyberattacks. For large companies, the situation is reversed, although they may not experience an increase in defence costs in the context of overall IT spending.

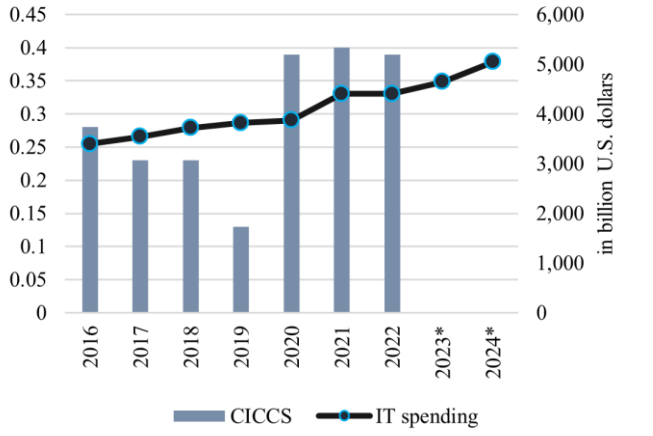

Fig. 5. Dynamics of the CICCS indicator and spending on information technologies for 2016-2024 (*2023 and 2024 contain forward estimates) (Statista, 2023b)

Comparing the costs of global cybersecurity with the needs of its development, one should note that during 2020-2021 needs prevailed over costs caused by the situation with COVID-19 (Figure 6). The year 2022 shows a balance between these indicators, which may indicate a calming of the fluctuations caused by the pandemic and the growth of companies' digitization.

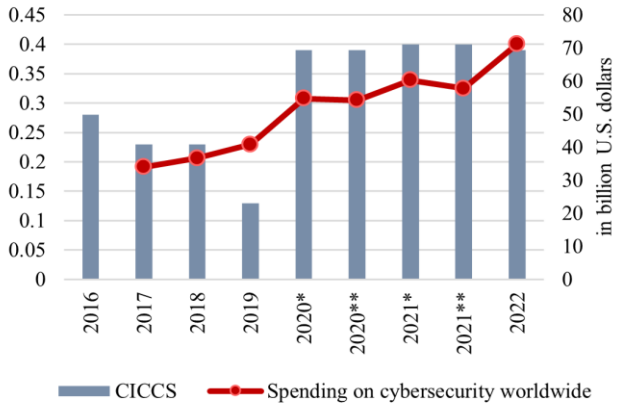

Fig. 6. Dynamics of the CICCS indicator and spending on global cyber security for 2016-2022 (*2020 and 2021 are the best-case scenarios considering COVID-19; **2020 and 2021 are the worst-case scenarios considering COVID-19) (Statista, 2023c)

The conducted comparative analysis of the needs for developing cybersecurity and directions that characterize the Industry 4.0 development allows us to draw the following conclusions. First, the active growth of modern technologies introduction requires creating a reliable cyber protection system. But this system has been significantly needed in the last three years, which requires more effective solutions. Second, IT and cybersecurity costs are growing in direct proportion to the growth of modern technologies. Although they did not cover the need for developing cybersecurity during the pandemic. The last year demonstrated a certain balance, which shows that companies understand the cyber threats that they face.

To create a balanced cyber system, it is necessary to consider that the internal and external business environment significantly affects its development and the development of enterprises as a whole (Brychko et al., 2023). At the same time, the digital achievements of companies are also a driver for the socio-economic development of countries (Melnyk et al., 2021b; Lieonov et al., 2022). On the one hand, they can act as tools for overcoming crises (Gurbanov et al., 2022). On the other hand, they can also lead to organizational mortality of companies (Dotsenko et al., 2023). Therefore, digital transformations require business reengineering, as it allows for a strategic approach to forming the cyber protection system of companies as a necessary link of these processes (Simion et al., 2018; Verboncu et al., 2018). It is also essential to identify "problem" areas of those business processes that require cyber protection in the first place (Cherchata et al., 2020). Creating and developing a company's cyber protection system is a painstaking process that requires not only digital transformations, the results of the scientific and technical process, but also complex measures related to the business processes of enterprises.

5. Summary and conclusion

Scientific and technological progress is an integral part of human development. Its results significantly affect companies' security systems due to the introduction of modern technologies reducing threats and risks related to disruption of production, logistics, technology and other processes. Cyber risks are the most unpredictable type of risks; therefore, creating a reliable and effective cybersecurity system is essential for ensuring the security of enterprises as a whole. This study aims to develop a composite indicator of business cybersecurity based on Porter's modified matrix approach. The proposed method and calculations make it possible to assess the need for developing the cybersecurity system of enterprises, considering the growth rate of cyber threats in the world and the level of cyber risks that they can cause.

The obtained results made it possible to form the following research conclusions. First, the world is witnessing rapid growth in the introduction and use of such modern technologies as artificial intelligence, blockchain technologies, industrial robots, IoT, etc. Actual and forecast empirical data confirm that there is currently an active phase of Industry 4.0 development. Secondly, applying the analysed technologies requires the improvement of cybersecurity measures, which involves creating a reliable and effective protection system for enterprises. Third, the calculation of companies' composite indicator of cybersecurity demonstrates a significant increase in their needs for cyber protection. First, this was caused by the COVID-19 pandemic, which led to increased cyber threats and cyber risks for enterprises. Fourth, the need for cyber protection prevails over the current state of technological development, although companies show full readiness to improve defence mechanisms, especially in cybersecurity. Fifth, spending on IT and cyber defence does not cover the growing need to counter cyber threats, although the last year has seen a balance between the two. It means that companies have demonstrated their understanding of the consequences of cyber threats and increased spending to ensure their countermeasures.

The main users of the proposed approach can be associations of enterprises in the cybersecurity industry, field associations, as well as individual enterprises, regardless of the scope and size of the activity. First, its use will contribute to forming an information base for assessing risks, needs and expectations regarding cybersecurity. Secondly, the obtained results will help form a strategy for developing the cybersecurity system for enterprises and individual industries. Thirdly, the proposed method will allow to quickly forecast the trends of the needs of companies in the development of cybersecurity to counteract the increase of unjustified costs in this direction.

Applying the proposed methodology for calculating the composite indicator of company cybersecurity may be associated with several limitations. The first concerns the singularity

of the matrix, which is formed as a matrix of indicators superposition that are components of the CICCS. In this case, its determinant will be zero, and the value of the composite indicator will also be zero. To overcome this limitation, it is necessary to monitor the input data used to build the matrix and, if necessary, replace or correct them. The second limitation relates directly to the form of presentation of CICCS component indicators. In their collection, it is essential to consider that they should characterize the survey results of the world's companies, regardless of their size or industry. Since the proposed method is universal, the CICCS calculation is also possible for companies of a separate sector. In this case, the collected data should reflect the survey results of only the companies from the analysed industry. That is, CICCS component indicators should be homogeneous. The third limitation concerns the need for constant monitoring and updating of the survey results, which are conducted by well-known cybersecurity expert companies. It is dictated by the fact that the composite indicator needs to be studied dynamically to form a more straightforward strategy for developing the company's cybersecurity system.

The future research directions can be the following ways. First, implementing technologies such as artificial intelligence, blockchains, the Internet of Things, industrial robots, etc., can be part of cybersecurity, reducing the risks of cyber threats. On the other hand, they can be the most vulnerable objects in companies and targeted by cyber criminals, which increases the cyber threat risks. Therefore, it is essential to investigate how these technologies affect the cyber defence of companies and what level of risk they can generate. Secondly, developing the methodology for determining the composite indicator of company cybersecurity proposed in the article for companies of different industries and sizes is advisable. It will allow them to reveal the level of cyber threats and risks and the degree of their need for cyber protection. The obtained results will contribute to forming strategic security solutions that more accurately correspond to the realities and needs of specific companies.

Acknowledgements

This research was performed within the framework of state budget research: No 0121U109559 “National security through the convergence of financial monitoring systems and cybersecurity: intelligent modeling of financial market regulation mechanisms”, No 0123U101945 “National security of Ukraine through the prevention of financial fraud and money laundering: war and post-war challenges”, No 0121U109553 “Convergence of economic and educational transformations in the digital society: modelling of the impact on regional and national security”.
The research received funding via the research subsidy of the Department of Applied Social Sciences of the Faculty of Organization and Management of the Silesian University of Technology in Poland for 2023, grant number 13/020/BK_23/0081. Publication supported by the pro-quality grant of the rector of the Silesian University of Technology, grant number: 13/020/RGJ22/0071

Reference

Akbarzadeh, A., Katsikas, S. K., 2023. Dependency-based security risk assessment for cyber-physical systems, International Journal of Information Security, 22(3), 563-578, DOI: 10.1007/s10207-022-00608-4

Alqudhaibi, A., Albarrak, M., Aloseel, A., Jagtap, S., Salonitis, K., 2023. Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations, Sensors, 23(9), 4539, DOI: 10.3390/s23094539

Alrumaih, T. N., Alenazi, M. J., 2023. Evaluation of industrial network robustness against targeted attacks, Concurrency and Computation: Practice and Experience, e7855, DOI: 10.1002/cpe.7855

Alzahrani, N. M., Alfouzan, F. A., 2022. Augmented reality (AR) and cybersecurity for smart cities – A systematic literature review, Sensors, 22(7), 2792, DOI: 10.3390/s22072792

Andrișan, G., Modreanu, A., 2022. An Overview of The Fourth Industrial Revolution through the Business Lens, Business Ethics and Leadership, 6(1), 39-46, DOI: 10.21272/bel.6(1).39-46.2022

Bac, T. P., Ha, D. T., Tran, K. D., Tran, K. P., 2023. Explainable Articial Intelligence for Cybersecurity in Smart Manufacturing, Artificial Intelligence for Smart Manufacturing: Methods, Applications, and Challenges, Cham: Springer International Publishing, 199-223, DOI: 10.1007/978-3-031-30510-8_10

Bozhenko, V., Mynenko, S., Shtefan, A., 2022. Financial Fraud Detection on Social Networks Based on a Data Mining Approach, Financial Markets, Institutions and Risks, 6(4), 119-124, DOI: 10.21272/fmir.6(4).119-124.2022

Brychko, M., Bilan, Y., Lyeonov, S., Streimikiene, D., 2023. Do changes in the business environment and sustainable development really matter for enhancing enterprise development?, Sustainable Development, 31(2), 587-599, DOI: 10.1002/sd.2410

Chen, Y., Xu, S., Lyulyov, O., Pimonenko, T., 2023. China’s digital economy development: incentives and challenges, Technological and Economic Development of Economy, 29(2), 518-538, DOI: 10.3846/tede.2022.18018

Cherchata, A., Popovychenko, I., Andrusiv, U., Simkiv, L., Kliukha, O., Horai, O., 2020. A methodology for analysis and assessment of business processes of Ukrainian enterprises, Management Science Letters, 10(3), 631-640, DOI: 10.5267/j.msl.2019.9.016

CyberEdge Group, 2022. Cyberthreat Defense Report, Retrieved from https://cyber-edge.com/cyberthreat-defense-report -2022/ (31.03.2023)

Dluhopolskyi, O., Pakhnenko, O., Lyeonov, S., Semenog, A., Artyukhova, N., Cholewa-Wiktor, M., Jastrzębski, W., 2023. Digital financial inclusion: COVID-19 impacts and opportunities, Sustainability (Switzerland), 15(3), DOI: 10.3390/su15032383

Dotsenko, T., Dvořák, M., Lyeonov, S., Kovács, A., 2023. Socially relevant factors of organizational mortality of enterprises: context of corporate sustainability in European countries, Economics and Sociology, 16(1), 284-299, DOI: 10.14254/2071-789X.2023/16-1/18

Fleck, A., 2022. Cybercrime Expected to Skyrocket in Coming Years, Retrieved from https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/ (31.03.2023)

Greenberg, A., 2018. The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (31.03.2023)

Gurbanov, N., Yagublu, N., Akbarli, N., Niftiyev, I., 2022. Digitalization and the COVID-19-led public crisis management: an evaluation of financial sustainability in the Azerbaijan business sector, SocioEconomic Challenges, 6(3), 23-38, DOI: 10.21272/sec.6(3).23-38.2022

Hope, A., 2022. Toyota’s Supply Chain Cyber Attack Stopped Production, Cutting Down a Third of Its Global Output, Retrieved from https://www.cpomagazine.com/cyber-security/toyotas-supply-chain-cyber-attack-stopped-production-cutting-down-a-third-of-its-global-output/ (31.03.2023)

IBM, 2022. Cost of a Data Breach Report 2022, Retrieved from https://www.ibm.com/reports/data-breach (31.03.2023)

Ievdokymov, V., Ostapchuk, T., Lehenchuk, S., Grytsyshen, D., Marchuk, G., 2020. Analysis of the impact of intangible assets on the companies' market value, Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 3, 164-170, DOI: 10.33271/nvngu/2020-3/164

Juma, M., Alattar, F., Touqan, B., 2023. Securing Big Data Integrity for Industrial IoT in Smart Manufacturing Based on the Trusted Consortium Blockchain (TCB), IoT, 4(1), 27-55, DOI: 10.3390/iot4010002

Kobis, P., Karyy, O. (2021). Impact of the human factor on the security of information resources of enterprises during the COVID-19 pandemic. Polish Journal of Management Studies, 24(2), 210-227. DOI: 10.17512/pjms.2021.24.2.13

Kolosok, S., Lyeonov, S., Voronenko, I., Goncharenko, O., Maksymova, J., Chumak, O., 2022. Sustainable business models and IT innovation: The case of the REMIT, Journal of Information Technology Management, 14, 147-156, DOI: 10.22059/JITM.2022.88894

Kuzior, A.,Sira, M., 2022. A Bibliometric Analysis of Blockchain Technology Research Using VOSviewer. Sustainability, 2022, 14(13), 8206, DOI: 10.3390/su14138206

Kuzior, A., Kwilinski, A., Tkachenko, V., 2019. Sustainable development of organizations based on the combinatorial model of artificial intelligence. Entrepreneurship and Sustainability Issues, 7 (2), 1353-1376, DOI: 10.9770/jesi.2019.7.2(39)

Kuzior, A.,Sira, M., Brożek, P. 2023. Use of Artificial Intelligence in Terms of Open Innovation Process and Management. Sustainability, 15(9), 7205, DOI: 10.3390/su15097205

Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., Brożek, P., 2022. Global digital convergence: Impact of cybersecurity, business transparency, economic transformation, and AML efficiency, Journal of Open Innovation: Technology, Market, and Complexity, 8(4), DOI: 10.3390/joitmc8040195

Kuzmenko, O., Kubálek, J., Bozhenko, V., Kushneryov, O., Vida, I. (2021). An approach to managing innovation to protect financial sector against cybercrime. Polish Journal of Management Studies, 24(2), 276-291.133–138, DOI: 10.17512/pjms.2021.24.2.17

Kuzmenko, O., Šuleř, P., Lyeonov, S., Judrupa, I., Boiko, A., 2020. Data mining and bifurcation analysis of the risk of money laundering with the involvement of financial institutions, Journal of International Studies, 13(3), 332-339, DOI: 10.14254/2071-8330.2020/13-3/22

Kwilinski, A., Kuzior, A. 2020. Cognitive Technologies in the Management and Formation of Directions of the Priority Development of Industrial Enterprises. Management Systems in Production Engineering, 28(2), DOI: 10.2478/mspe-2020-0020

Lakshmanan, R., 2022. Indian Energy Company Tata Power's IT Infrastructure Hit By Cyber Attack, Retrieved from https://thehackernews.com/2022/10/indian-energy-company-tata-powers-it.html (31.03.2023)

Lampropoulos, G., Siakas, K., 2023. Enhancing and securing cyber-physical systems and Industry 4.0 through digital twins: A critical review, Journal of Software: Evolution and Process, 35(7), e2494, DOI: 10.1002/smr.2494

Lieonov, S., Hlawiczka, R., Boiko, A., Mynenko, S., Garai-Fodor, M., 2022. Structural modelling for assessing the effectiveness of system for countering legalization of illicit money, Journal of International Studies, 15(3), 215–233, DOI: 10.14254/2071-8330.2022/15-3/15

Maple Leaf Foods, 2022. Maple Leaf Foods Confirms System Outage Linked to Cybersecurity Incident, Retrieved from https://www.mapleleaffoods.com/news/system-outage-linked-to-cybersecurity-incident/ (31.03.2023)

Masood, A. B., Hasan, A., Vassiliou, V., Lestas, M., 2023. A Blockchain-Based Data-Driven Fault-Tolerant Control System for Smart Factories in Industry 4.0, Computer Communications, 204, 158-171, DOI: 10.1016/j.comcom.2023.03.017

Melnyk, L., Kubatko, O., Matsenko, O., Balatskyi, Y., Serdyukov, K., 2021a. Transformation of the human capital reproduction in line with Industries 4.0 and 5.0, Problems and Perspectives in Management, 19(2), 480-494, DOI: 10.21511/ppm.19(2).2021.38

Melnyk, L., Kubatko, O., Piven, V., Klymenko, K., Rybina, L., 2021b. Digital and economic transformations for sustainable development promotion: A case of OECD countries, Environmental Economics, 12(1), 140-148, DOI: 10.21511/EE.12(1).2021.12

Michael, P., 2023. Technology statistics: How fast is Tech advancing? [growth charts] 2023, Retrieved from https://mediapeanut.com/how-fast-is-technology-growing-statistics-facts/ (31.03.2023)

Muradov, İ., 2022. Problems of E-Governance in Government Agencies and their Solutions, SocioEconomic Challenges, 6(1), 79-86, DOI: 10.21272/sec.6(1).79-86.2022

Pakhnenko, O., Kuan, Z., 2023. Ethics of Digital Innovation in Public Administration, Business Ethics and Leadership, 7(1), 113-121, DOI: 10.21272/bel.7(1).113-121.2023

Pakhnenko, O., Pudło, T., 2023. HealthTech in ensuring the resilience of communities in the post-pandemic period, Health Economics and Management Review, 4(2), 31-39, DOI: 10.21272/hem.2023.2-03

Rahmanov, F., Salahov, R., Hashimova, A., 2023. Management of Digitisation Processes in the Field of Social Services, Marketing and Management of Innovations, 14(2), 174-184, DOI: 10.21272/mmi.2023.2-16

Rapp, N., Hackett, R., 2017. A Hacker's Tool Kit, Retrieved from https://fortune.com/2017/10/25/cybercrime-spyware-marketplace/ (31.03.2023)

Rekunenko, I., Boiko, A., Kramarenko, O., Khan, B., 2022. Data Management in Healthcare Research as a Guarantee of its Quality, Health Economics and Management Review, 3(2), 36-43, DOI: 10.21272/hem.2022.2-04

Reputiva, 2022. Key Takeaways: Statista's In-depth: Industry 4.0 2021: Digital Market Outlook, Retrieved from https://www.reputiva.com/key-takeaways-statistas-in-depth-industry-4-0-2021-digital-market-outlook/ (31.03.2023)

Rika, M., 2023. Robots Among Us – The Global Robotics Market Growing Rapidly, Retrieved from https://statzon.com/insights/global-robotics-market-growing-rapidly (31.03.2023)

Samusevych, Y. V., Novikov, V. V., Artyukhov, A. Y., Vasylieva, T. A., 2021. Convergence trends in the "Economy - Education - Digitalization - National Security" chain, Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 6, 177-183, DOI: 10.33271/NVNGU/2021-6/177

Schwab, K., 2016. The Fourth Industrial Revolution, Retrieved from https://law.unimelb.edu.au/__data/assets/pdf_file/0005/3385454/Schwab-The_Fourth_Industrial_Revolution_Klaus_S.pdf (31.03.2023)

Sergiienko, L., Polyak, K., Poverlyak, T., Cherchata, A., Andriushchenko, I., Zhyliakova, O., 2020. Application of taxonomic analysis in assessing the level of enterprise development in emergency situations, Management Science Letters, 10(6), DOI: 10.5267/j.msl.2019.11.024

Sidelnyk, N. Y., 2023. Development of insurance in the context of innovative socio-economic transformations: PhD thesis: 072. Sumy State University, Sumy, Ukraine.

Simion, C.-P., Verboncu, I., Şavga, L., 2018. Project Portfolio Management in Romanian R&D Organizations, The 32nd International Business Information Management Association Conference, IBIMA 2018 - Vision 2020: Sustainable Economic Development and Application of Innovation Management from Regional expansion to Global Growth, Seville, 4054-4062.

Skliar, I. D., Samoilikova, A. V., 2014. Risk evaluation at enterprise innovation and investment activity financing, Actual Problems of Economics, 161(11), 173-178.

Skrynnyk, O., 2023. Prediction of Convergent and Divergent Determinants of Organisational Development, Business Ethics and Leadership, 7(1), 74-81, DOI: 10.21272/bel.7(1).74-81.2023

Statista, 2022a. Estimated worst potential loss in value due to a cyber incident according to senior executives worldwide as of February 2018, by company revenue size, Retrieved from https://www.statista.com/statistics/881519/estimated-worst-potential-loss-value-cyber-incident-company-revenue-size/ (31.03.2023)

Statista, 2022b. Revenues from the artificial intelligence (AI) software market worldwide from 2018 to 2025, Retrieved from https://www.statista.com/statistics/607716/worldwide-artificial-intelligence-market-revenues/ (31.03.2023)

Statista, 2022c. Size of the blockchain technology market worldwide from 2018 to 2025, Retrieved from https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/ (31.03.2023)

Statista, 2023a. Global industry sectors most targeted by basic web application attacks from November 2021 to October 2022, Retrieved from https://www.statista.com/statistics/221293/cyber-crime-target-industries/#statisticContainer (31.03.2023)

Statista, 2023b. Information technology (IT) worldwide spending from 2005 to 2024, Retrieved from https://www.statista.com/statistics/203935/overall-it-spending-worldwide/ (31.03.2023)

Statista, 2023c. Spending on cybersecurity worldwide from 2017 to 2022, Retrieved from https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/ (31.03.2023)

Tatli, H. S., Yavuz, M. S., Ongel, G., 2023. The Mediator Role of Task Performance in the Effect of Digital Literacy on Firm Performance, Marketing and Management of Innovations, 14(2), 75-86, DOI: 10.21272/mmi.2023.2-08

Topcuoglu, E., Oktaysoy, O., Uygungil-Erdogan, S., Kaygin, E., Karafakioglu, E., 2023. The Mediating Role of Job Security in The Impact of Digital Leadership on Job Satisfaction and Life Satisfaction, Marketing and Management of Innovations, 1, 122-132, DOI: 10.21272/mmi.2023.1-11

Vasilyeva, T., Kuzmenko, O., Stoyanets, N., Artyukhov, A., Bozhenko, V., 2022. The depiction of cybercrime victims using data mining techniques, Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 5, 174-178, DOI: 10.33271/nvngu/2022-5/174

Verboncu, I., Şavga, L., Simion, C. P., 2018. Managerial reengineering and efficiency, The 32nd International Business Information Management Asso-ciation Conference, IBIMA 2018 - Vision 2020: Sustainable Economic Development and Application of Innovation Management from Regional expansion to Global Growth, Seville, 4045-4053.

Wang, Z., Lin, S., Chen, Y., Lyulyov, O., Pimonenko, T., 2023. Digitalization Effect on Business Performance: Role of Business Model Innovation, Sustainability, 15(11), 9020, DOI: 10.3390/su15119020

World Economic Forum, 2023. The Global Risks Report 2023 18th Edition, Retrieved from https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf?_gl=1*b8k930*_up*MQ..&gclid=Cj0KCQjw4s-kBhDqARIsAN-ipH0GJ_KEe3g7TllDlfjkfZYkSDl oZdCTiyNtIbwd FolQsKTBQL_ycFAaAlyCEALw_wcB (31.03.2023)

Yarovenko, H., Rogkova, M., 2022. Dynamic and bibliometric analysis of terms identifying the combating financial and cyber fraud system, Financial Markets, Institutions and Risks, 6(3), 93-104, DOI: 10.21272/fmir.6(3).93-104.2022

Appendix

Appendix A

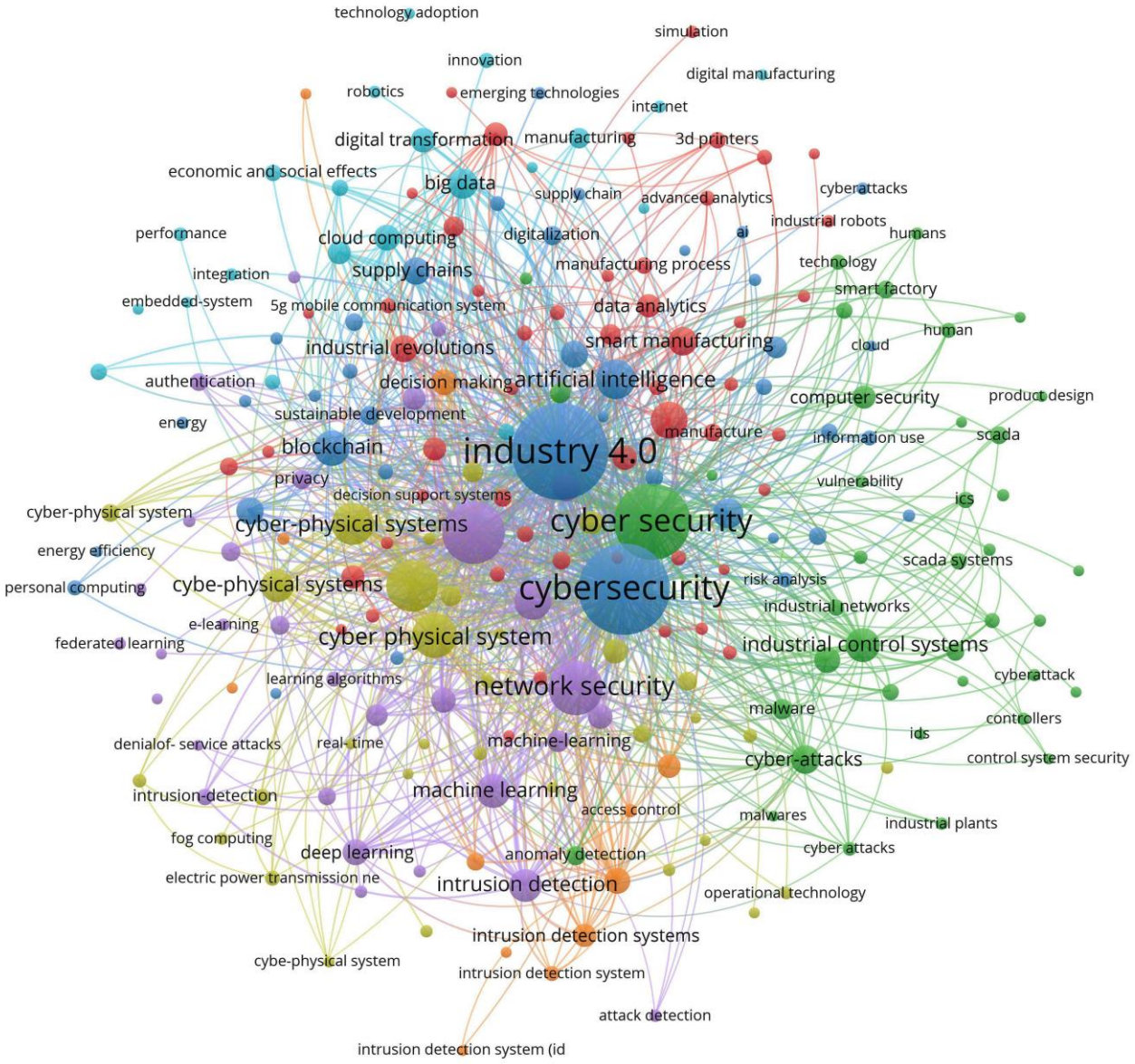

Fig. 1. Results of a bibliometric analysis of scientific research devoted to cybersecurity issues in the context of Industry 4.0

Appendix B

Table 1. Information base of CICCS formation for 2014-2022 (IBM, 2022; CyberEdge Group, 2022)

Indicator	2014	2015	2016	2017	2018	2019	2020	2021	2022
Share of organizations that experienced at least one successful cyberattack, %	61.9	70.5	75.6	79.2	77.2	78.0	80.7	86.2	85.3
Share of organizations that experienced six or more successful cyberattacks, %	16.2	22.6	23.8	32.9	27.4	31.5	35.2	39.7	40.7
Share of respondents who believe that a successful cyberattack on their organization in the next 12 months will be "likely", %	38.1	51.9	62.1	61.5	62.3	65.2	69.3	75.6	76.1
Share of respondents who believe that a successful cyberattack on their organization in the next 12 months will be "very likely", %	8.5	14.0	16.1	20.4	19.7	21.2	27.2	32.0	35.1
The threat index, reflecting the general concern about cyberattacks, units	3.61	3.26	3.71	3.75	3.54	3.52	3.79	3.88	3.88
Security Concern Index, unit	2.94	2.99	3.37	3.41	3.18	3.19	3.53	3.65	3.64
Share of organizations with a growing security budget, %	-	-	-	76.0	78.7	83.5	85.4	77.8	83.2
Share of organizations experiencing a shortage of qualified IT security personnel, %	-	-	-	-	80.9	84.2	84.8	87.0	84.1
Share of organizations affected by ransomware, %	-	-	-	-	55.1	56.1	62.4	68.5	71.0
Share of stolen or compromised credentials, million US dollars	-	-	3.62	3.86	3.92	3.95	4.24	4.35	3.62

Table 2. Normalized values of indicators that are components of CICCS for 2016-2022 (Sidelnyk, 2023)

Indicator	2016	2017	2018	2019	2020	2021	2022
Share of organizations that have experienced at least one successful cyber attack	1.00	0.66	0.85	0.77	0.52	0.00	0.08
Share of organizations that have experienced six or more successful cyber attacks	1.00	0.46	0.79	0.54	0.33	0.06	0.00
Share of respondents who believe a successful cyberattack on their organization in the next 12 months is "likely"	0.96	1.00	0.95	0.75	0.47	0.03	0.00
Share of respondents who believe a successful cyberattack on their organization in the next 12 months is "very likely"	1.00	0.77	0.81	0.73	0.42	0.16	0.00
A threat index that reflects the general concern about cyber attacks	0.47	0.36	0.94	1.00	0.25	0.00	0.00
Security Concern Index	0.60	0.51	1.00	0.98	0.26	0.00	0.02
Share of organizations with growing security budgets	0.00	0.13	0.38	0.82	1.00	0.29	0.80
The share of organizations experiencing a shortage of qualified IT security personnel	1.00	0.90	0.80	0.37	0.29	0.00	0.38
Share of organizations affected by ransomware	1.00	0.86	0.71	0.66	0.38	0.11	0.00
Share of stolen or compromised credentials	1.00	0.67	0.59	0.55	0.15	0.00	1.00

Appendix C

Table 3. Growth rates of CICCS constituent indicators for 2014-2022 (Sidelnyk, 2023)

Indicator	2016	2017	2018	2019	2020	2021	2022
Share of organizations that have experienced at least one successful cyber attack	7%	5%	-3%	1%	3%	7%	-1%
Share of organizations that have experienced six or more successful cyber attacks	5%	38%	-17%	15%	12%	13%	3%
Share of respondents who believe a successful cyberattack on their organization in the next 12 months is "likely"	20%	-1%	1%	5%	6%	9%	1%
Share of respondents who believe a successful cyberattack on their organization in the next 12 months is "very likely"	15%	27%	-3%	8%	28%	18%	10%
A threat index that reflects the general concern about cyberattacks	14%	1%	-6%	-1%	8%	2%	0%
Security Concern Index	13%	1%	-7%	0%	11%	3%	0%
Share of organizations with growing security budgets	1%	2%	4%	6%	2%	-9%	7%
The share of organizations experiencing a shortage of qualified IT security personnel	1%	1%	1%	4%	1%	3%	-3%
Share of organizations affected by ransomware	7%	7%	7%	2%	11%	10%	4%
Share of stolen or compromised credentials	0%	7%	2%	1%	7%	3%	-17%

Appendix D

Table 4. Superposition matrix of indicators that are components of CICCS (Sidelnyk, 2023)

Level of cyber risk / Growth rate of cyber threats	Critical	High	Average	Low
Anticipatory growth	b_{11}	b_{12}	b_{13}	b_{14}
Rapid growth	b_{21}	b_{22}	b_{23}	b_{24}
Moderate growth	b_{31}	b_{32}	b_{33}	b_{34}
Falling growth	b_{41}	b_{42}	b_{43}	b_{44}

Appendix E

Table 5. Adjusted superposition matrix of CICCS components for 2016 (Sidelnyk, 2023)

2016		The lower / upper limit of the cyber risk level			
		0.75 / 1	0.6 / 0.75	0.25 / 0.6	0 / 0.25
The lower / upper limit of the growth rate of cyber threats	16 / –	2	1	1	1
	10 / 16	2	1	3	1
	8 / 10	1	1	1	1
	– / 8	6	1	1	2

Table 6. Adjusted superposition matrix of CICCS components for 2017 (Sidelnyk, 2023)

2017		The lower / upper limit of the cyber risk level			
		0.75 / 1	0.5 / 0.75	0.25 / 0.5	0 / 0.25
The lower / upper limit of the growth rate of cyber threats	19 / –	2	1	2	1
	9 / 19	1	1	1	1
	0 / 9	3	4	2	2
	– / 0	2	1	1	1

Table 7. Adjusted superposition matrix of CICCS components for 2018 (Sidelnyk, 2023)

2018		The lower / upper limit of the cyber risk level			
		0.75 / 1	0.5 / 0.75	0.25 / 0.5	0 / 0.25
The lower / upper limit of the growth rate of cyber threats	3.5 / –	1	2	2	1
	0 / 3.5	3	2	1	1
	-2 / 0	1	1	1	1
	– / -2	6	1	1	1

Table 8. Adjusted superposition matrix of CICCS components for 2019 (Sidelnyk, 2023)

2019		The lower / upper limit of the cyber risk level			
		0.75 / 1	0.5 / 0.75	0.25 / 0.5	0 / 0.25
The lower / upper limit of the growth rate of cyber threats	7.5 / –	1	3	1	1
	4 / 7.5	2	2	1	1
	0 / 4	3	3	2	1
	– / 0	2	1	1	1

Table 9. Adjusted superposition matrix of CICCS components for 2020 (Sidelnyk, 2023)

2020		The lower / upper limit of the cyber risk level			
		0.75 / 1	0.5 / 0.75	0.25 / 0.5	0 / 0.25
The lower / upper limit of the growth rate of cyber threats	14 / –	1	1	2	1
	8 / 14	1	1	3	2
	2 / 8	1	2	2	3
	– / 2	2	1	2	1

Table 10. Adjusted superposition matrix of CICCS components for 2021 (Sidelnyk, 2023)

2021		The lower / upper limit of the cyber risk level			
		0.225 / 0.3	0.15 / 0.225	0.075 / 0.15	0 / 0.075
The lower / upper limit of the growth rate of cyber threats	10 / –	1	2	1	2
	6 / 10	2	1	2	2
	0 / 6	1	1	1	5
	– / 0	2	1	1	1

Table 11. Adjusted superposition matrix of CICCS components for 2022 (Sidelnyk, 2023)

2022		The lower / upper limit of the cyber risk level			
		0.75 / 1	0.5 / 0.75	0.25 / 0.5	0 / 0.25
The lower / upper limit of the growth rate of cyber threats	8 / –	1	1	1	2
	0 / 8	2	1	1	4
	-8 / 0	2	1	2	3
	– / -8	2	1	1	1

公司网络安全系统：评估、风险和期望

關鍵詞
网络安全
网络风险
网络威胁
工业4.0
波特法

摘要
工业 4.0 的后果对网络犯罪的增长产生了不利的副作用，这需要为公司创建有效的网络安全系统。 因此，本研究旨在制定企业网络安全综合指标来评估其发展需求。 为此，作者对波特方法进行了修改，根据网络威胁和风险的增长率构建叠加矩阵，计算其定量特征和综合指标。 这些计算基于 2016 年至 2022 年描述网络安全漏洞和网络威胁后果的指标：经历一次、六次或更多成功网络攻击的公司比例，考虑到未来 12 个月内网络攻击成功的可能性和极有可能，安全威胁和担忧指数、受勒索软件影响且安全预算不断增长且缺乏熟练 IT 安全人员的公司比例、凭据被盗或泄露的成本。 因此，2020-2022 年网络安全需求显着增加，这主要是由于数字化转型和 COVID-19 大流行后网络威胁的增长。 对拟议指标与工业4.0发展特征的比较分析表明，对可靠的网络安全系统的需求比现代技术的积极发展更为重要。 IT支出也在增加，但不足以满足网络安全发展的需求，除了2022年的结果。 拟议的指标是为全球公司定义的，但其多功能性使得该方法可以应用于不同行业和规模的企业。