Financial Markets, Institutions and Risks, Volume 4, Issue 3, 2020
ISSN (online) – 2521-1242 ISSN (print) – 2521-1250

ARMG Publishing
"Thinking ahead"

Strategy for Determining Country Ranking by Level of Cybersecurity

http://doi.org/ 10.21272/fmir.4(3).124-137.2020

Hanna Yarovenko, ORCID: https://orcid.org/0000-0002-8760-6835

PhD, Associate Professor of the Economic Cybernetics Department, Sumy State University, Sumy, Ukraine

Olha Kuzmenko, ORCID: https://orcid.org/0000-0001-8520-2266

Doctor of Economics. Professor. Head of Economic Cybernetics Department, Sumy State University. Head of Scientific and Educational Center for Business Analytics, Sumy, Ukraine

Mario Stumpo, ORCID: https://orcid.org/0000-000151326041

Founder and CEO of Yanda.io, Italy

Abstract

The rapid development of the fourth industrial revolution contributed to the growth of computerization and digitalization of many spheres of society, which eventually led to the emergence of cybercrime. As a result, it is necessary to develop a cybersecurity strategy at the country level, which involves the development of effective measures to protect information. The purpose of this article is to determine the strategy for ranking countries by their level of cybersecurity. For its implementation, 12 indicators were selected that characterize various aspects of cybersecurity of countries: Cyber Security Policy Development, Cyber Threat Analysis and Information, Education and Professional Development, Contribution to global cyber security, Protection of digital services, Protection of essential services, E-identification and trust services, Protection of personal data, Cyber incidents response, Cyber crisis management, Fight against cybercrime, Military cyber operations. Their actual values were taken for 160 countries in 2018. The article proved that the existing method of determining the actual ranking of countries has a number of shortcomings, which are the lack of solutions to problems related to the dimensionality of data, determining the weights of the analyzed indicators, taking into account the diversity of indicators and their fundamental differences. To avoid these shortcomings, it is proposed to use multi-attribute decision-making methods, which are used in the decision-making process, but their capabilities allow the evaluation of ratings. The methods of TOPSIS, VIKOR and MAAM were used in the article. As a result, it was found that the rating by the MAAM method has about 25% similarity with the values of the ranking. Also, this method has most of the disadvantages inherent in the actual. The TOPSIS and VIKOR methods showed better results, which were less similar to the real values. It was found that VIKOR (v = 0.5) shows more balanced estimates than VIKOR (v = 1.0) in relation to the ranking of countries in terms of cybersecurity. VIKOR (v = 1.0) is more suitable for solving the problem of choosing alternatives than for rating. The TOPSIS method proved to be the most effective for ranking countries, which eliminates the shortcomings of the real assessment method and allows to determine the best and worst alternative, which facilitates the analysis separately for the indicators. Checking the effectiveness of the obtained ratings, using Spearman's rank correlation coefficient, proved their effectiveness.

Keywords: country, cybersecurity, MAAM, National Cybersecurity Index, rank, strategy, TOPSIS, VIKOR.

JEL Classification: D80, O30

Cite as: Yarovenko, H., Kuzmenko, O., Stumpo, M., (2020). Strategy for Determining Country Ranking by Level of Cybersecurity. *Financial Markets, Institutions and Risks*, *4*(3), 124-137. http://doi.org/ 10.21272/fmir.4(3).124-137.2020.

Introduction

The rapid development of new information technologies, computerization and digitalization of many spheres of society have led to an increase in cybercrime in the world. This is manifested in the implementation of mass hacking attacks, as a result of which companies lose a large amount of information about customers, financial transactions, classified information. Also, the number of viral messages, the action of which leads to malfunctions of software and hardware. New methods of cyber-fraud are appearing regularly, aimed at obtaining various types of information from users. Cybercriminals have also begun to interfere in the work of state bodies, which leads to the emergence of cyberwar between states, the emergence of information crises, and so on. This problem has become large-scale, which requires the development and implementation of more effective solutions to the struggle at the state level.

One of these areas is the formation of an effective cyber security strategy of the country, which should include a system of measures related to the organization of relevant institutions and bodies whose activities are aimed at ensuring cyber security. The strategy should also cover the following areas: cybersecurity policy making, development of appropriate legal framework, educational programs, cybercrime liability system, investment in cybersecurity research, development of powerful cyberphysical systems, software for monitoring, prevention and detection of cybercrime, etc. In developing a strategy, it is important to understand which aspects of a country's cybersecurity need to be improved and strengthened, and which already have a strong basis and require support. This can be assessed in the process of determining the ranking of countries, which is formed by the level of cybersecurity.

There are several indicators used to rank countries, including the National Cybersecurity Index, which assesses the level of readiness of countries to counter cyber threats. To calculate it, a number of indicators are used that relate to various aspects of cybersecurity: legal, organizational, technical, educational, etc. After receiving their estimates, a generalized indicator is calculated by finding the share of the total score for the country from the total maximum score. But this approach does not take into account the importance of indicators in the process of forming an overall rating, does not respond to cases where they have different amplitudes of values, and does not involve the use of additional characteristics that would help clearly see deviations from actual maximum scores. Therefore, the use of different approaches, such as, for example, multicriteria analysis of decisions, will allow the assessment of ratings more carefully, because they eliminate these shortcomings. Although these methods are used in the selection and decision-making process, they allow to effectively evaluate the objects of study. The choice of assessment method can significantly affect the formation of a cybersecurity strategy for the country, so it is necessary to understand the effectiveness of the method and its additional capabilities.

1. Literature Review

In recent decades, the number of scientific studies on cybersecurity problems has increased. Several can be identified, which focus on the formation of a security strategy at the country level. Thus, Ghernouti-Hélie (2010) explores some issues related to the deployment of a national cybersecurity strategy for the country in the context of its interaction with other countries. Galinec et al. (2017) on the example of the National CyberSecurity Strategy of the Republic of Croatia and the Action Plan try to identify organizational problems in the process of their formation and provide recommendations for their solution. Teoh and Mahmood (2017) examines the relationship between national cybersecurity strategies and the digital economy and analyzes their impact on the success of the digital economy. Kshetri and Murugesan (2013) highlight key elements of national cybersecurity strategies and assess their impact locally, nationally and globally. Kostyuk (2014) explores the challenges facing countries in the context of the creation of an effective national cybersecurity system and emphasizes the need to develop a private-public partnership in this area. This aspect is also considered by Štitilis et al. (2017), which analyzes national cybersecurity strategies for their compliance with cybersecurity policies and strategic areas of the EU and NATO. Jacobs et al. (2017) proposes as part of the country's cybersecurity strategy to create a cyber defense monitoring and incident response model based on integrating the country's military capabilities and cybersecurity operational models.

An important direction in the development of cybersecurity of the country is the use of modern methods and tools that are aimed at improving its effectiveness. Thus, Kolini and Janczewski (2017) explore the possibilities of using mathematical methods to improve the effectiveness of information protection strategies, namely they highlight cluster analysis and thematic modeling. Fenton and Neil (2012) examines the areas of bayesov's use of cause-and-effect risk models in its assessment process to ensure more effective management and process of rattling cyber defence decisions. Noel et al. (2016) is reviewing the CyGraph system, which is a unified graphical cybersecurity model whose goal is to provide a response to potential and real cyberattacks. Zhang et al. (2019) is exploring blockchain technology capabilities to ensure security and privacy in cryptocurrency systems. Some researchers pay attention to the development of specialized information systems, which involve automation of current business processes, which prevents external interference in their implementation (Yarovenko, 2004).

Multi-attribute decision-making methods are used to solve various kinds of tasks. Thus, Akram et al. (2019) paid attention to the VIKOR methodology for its evaluation capabilities for the selection of waste treatment methods and the site to plant a thermal power station. Ghaleb et al. (2020) conducted a comparative analysis of MCDM approaches to select production processes. Mardani et al. (2016) explored the possibilities of using VIKOR Technique in areas such as sustainability and renewable energy. Suniantara and Putra (2019) conducted a comparative characteristic of VIKOR and TOPSIS Methods in order to select significant variables in the process of variable reactions of brightness and tenderness in the process of making envelopes. Chatterjeea and Chakraborty (2016) assessed the effectiveness of abrasive materials based on seven criteria, during which the VIKOR method and its various modifications were applied. That is, multi-attribute decision-making methods are widely used regardless of the object of research, so they can be used to rank countries on the level of their cybersecurity.

Thus, despite significant scientific achievements to solve the problem of cybersecurity, there are a number of issues that are quite weakly represented by scientific works of specialists. This also applies to the development of an effective system for evaluating countries in terms of their cybersecurity, which will contribute to the development of a powerful national strategy of the country in the future.

2. Data and Methodology

2.1. Data. To conduct the study, 12 indicators were taken that characterize various aspects of the country's cybersecurity, used to determine the National Cybersecurity Index and the corresponding country rating. Thus, the empirical database was formed (e-Governance Academy Foundation, 2020):

1) Cyber Security Policy Development characterizes the general level of cybersecurity policy in the country, which is manifested in the creation of relevant groups and alliances on this issue, ensuring their coordination, development of strategy and plan for the implementation of cybersecurity;
2) Cyber Threat Analysis and Information reflects the areas related to the formation of information support on cybersecurity, which includes annual reporting on cyber threats in the world and the development of special web resources, as well as areas for the creation and development of specialized think tanks analysis of the state of cybersecurity in the world;
3) Education and Professional Development characterizes the level of education in the field of cybersecurity, which is manifested in the definition of competencies in this area for different levels of education: primary, secondary, bachelor’s, master’s, PhD, and provides for the creation of a professional cybersecurity association. this problem;
4) Contribution to global cyber security reflects the areas related to the country’s activities at the global level to form its contribution to the development of the Convention on Cybercrime, international missions, cybersecurity organizations, as well as to build opportunities to build cybersecurity capacity for other countries;
5) Protection of digital services provides an assessment of the country’s actions to ensure accountability for digital service providers, the development of cybersecurity standards for the public sector and the formation of special competent oversight bodies;
6) Protection of essential services characterizes the country’s measures to identify operators of basic services, develop requirements for them, create a competent supervisory authority in this area, the implementation of regular monitoring of security measures in the process of basic services;
7) E-identification and trust services reflect the actions of the state to create unique identifiers, competent supervisory authorities, develop requirements for cryptosystems, electronic identification and signature;
8) Protection of personal data refers to areas related to the formation of effective legislation in the field of personal data protection and the establishment of appropriate bodies;
9) Cyber incidents response involves the country’s actions to form special units to respond to cyber incidents, a single point of contact for international coordination, the development of a system of responsibility for reporting cases of cybercrime;
10) Cyber crisis management includes issues related to the formation of a cyber crisis management plan at the national level; participation in international exercises on cybercrisis; operational support of volunteers during the cyber crisis;

11) Fight against cybercrime characterizes aspects of the activities of specialized units on cybercrime, digital forensics, contact point on international cybercrime;
12) Military cyber operations refers to areas for specialized cyber operations and the country's participation in international cyber exercises.

Data indicators were taken for 160 countries in 2018 (e-Governance Academy Foundation, 2020). All values are measured in equal values from 0 to 10 and represent estimates that are provided to each country based on the information provided by it.

2.2. Methodology. The study selected Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS), which belongs to the class of multicriteria problems and was developed by Ching-Lai Hwang and Yoon in 1981 (Hwang and Yoon, 1981). In the following years, this technique was further developed and improved. Its basic idea is to identify two alternatives, one of which has the smallest geometric distance to a positive ideal solution and the other has the largest geometric distance to a negative ideal solution. As a result, the method allows to determine the relative distance to the ideal solution, which helps to obtain an overall score for each alternative, which can act as its rating. TOPSIS provides for the following steps.

At the first stage, a matrix of m-alternatives and n-criteria is created. Alternatively, we choose the countries for which it is necessary to determine the rating. The indicators will be cybersecurity indices, which were described in section 2.1.

At the second stage, the normalized values of cybersecurity indicators are determined. The initial data are reduced to dimensionless quantities, ie normalized, because their values may be incomparable. Formula 1 is used for this step:

$$u_{ij} = \frac{a_{ij}}{\sqrt{\sum_{j=1}^{n} a_{ij}^2}}, \tag{1}$$

where u_{ij} – normalized values of individual cybersecurity indicators for *i*-country ($i = 1 \div m; j = 1 \div n$);

m – the number of alternatives, in our case equal to the number of countries ($m = 160$);

n – the number of alternatives, in our case equal to the number of countries ($n = 12$);

a_{ij} – the actual value of a separate cybersecurity indicator for *i*- country.

At the third stage the weighted normalized matrix of decisions in which weight of a separate indicator for decision-making concerning a rating of the country (Formula 2) is defined:

$$x_{ij} = w_j \cdot u_{ij}, \tag{2}$$

where x_{ij} - weighted normalized values of individual cyber security indicators for *i*-country ($i = 1 \div m; j = 1 \div n$);

w_j – the weight of each j- target function, which reflects the importance of the cybersecurity indicator for the overall ranking of the country, with $\sum_{j=1}^{n} w_j = 1$. In our case, the weight was defined as the share of the normative value of the j-th indicator in their total score (Formula 3):

$$w_j = \frac{w_j^*}{\sum_{j=1}^{n} w_j^*}, \tag{3}$$

where w_j^* – normative assessment of the j-indicator of cybersecurity.

At the fourth stage, a positive and negative ideal solution is determined, ie the country with the highest level of cybersecurity and the country with the worst performance are determined (formulas 4-5):

$$A^+ = \{x_1^+, \dots, x_n^+\}, \\ x_j^+ = \left\{\max_i x_{ij} | j \in C_j(max); \min_i x_{ij} | j \in C_j(min)\right\}, \tag{4}$$

$$A^- = \{x_1^-, \dots, x_n^-\}, \\ x_j^- = \left\{\min_i x_{ij} | j \in C_j(min); \max_i x_{ij} | j \in C_j(max)\right\}, \tag{5}$$

where A^+ and A^- – respectively, the best and worst alternatives or positive and negative ideal solutions, which are represented by a set of cybersecurity indicators;

x_j^+ – calculated maximum values for those criteria that positively affect the formation of the best alternative, or minimum values that also have a positive impact;

x_j^- – calculated minimum values for those criteria that negatively affect the formation of the worst alternative, or maximum values that also have a negative impact;

C_j – a set of values for the j-indicator of cybersecurity.

The fifth stage is to estimate the distances for each country to the ideal alternative. The distance to the best (positive) alternative is calculated by formula 6 and its value for a particular *i*- country shows that the smaller it is, the closer the country is to the ideal values of safety indicators, and its rating will be higher. The distance to the worst (negative) alternative is determined by formula 7 and its value indicates that the smaller it is, the closer the country is to the worst-case scenario, ie it will have a low rating in terms of cybersecurity.

$$S_i^+ = \sqrt{\sum_{j=1}^{n}\left(x_{ij} - x_j^+\right)^2}, \tag{6}$$

$$S_i^- = \sqrt{\sum_{j=1}^{n}\left(x_{ij} - x_j^-\right)^2}, \tag{7}$$

where S_i^+ – the distance of the country's indicators to the best (positive) alternative;

S_i^- – the distance of the country's indicators to the worst (negative) alternative.

At the sixth stage, the calculation of the relative distance to the ideal alternative is carried out, which involves determining the similarity of the values of the criteria for each *i*- country with the worst condition (Formula 8):

$$Q_i = \frac{S_i^-}{S_i^+ + S_i^-} \tag{8}$$

If the obtained value of Q_i approaches 1, then this indicates that the i-and the country has the best combination of cybersecurity indicators, which is close to the ideal combination. If the value of Q_i approaches 0, then this indicates the worst combination of cybersecurity indicators and this country will have a rather low rating.

At the seventh stage, the rating is assessed by determining the rank for the calculated values. For this purpose, the countries are ranked according to the obtained Q and indicator in descending order. Then they are assigned a serial number in the row. If the values of Q and are the same, then the standardized rank for is calculated as the arithmetic mean of the ordinal numbers for the same Q and. To check the correctness of the ranks obtained, it is necessary to find their sum for the entire series and compare this value with N (N + 1)/2, where N is the number of countries in the series, that is, 160. The offensive method, which is used for carrying out projects, is the original VIKOR (Vlse Kriterijumska Optimizacija Kompromisno Resenje, in Serbian), which means multicriteria optimization and compromise solution. Winning proponent in 1979 by Serbian honored S. Opricovic, and internationally acknowledged classical version in publication Opricovic and Tzeng (2004). The essence of the method of polarity is in the knowledge of various critical criteria, as it is known as the world of proximity to the ideal compromise solution. VIKOR is a very comprehensive VIKOR, fuzzy VIKOR, regret theory based VIKOR, modified VIKOR and interval VIKOR, or for typical tasks we can choose original VIKOR, published by Chatterjee and Chakraborty (2016). Realization of the given method of transferring the offensive stages.

At the first stage, there is a matrix of alternatives and criteria, like є an analogous matrix, created by the TOPSIS method.

At the second stage, normalization of cob indicators in cybersecurity, presented in the matrix view, is carried out. At the same time, it is considered the fact in the flow of the exponent. If the value of the injection is positive, then it is a stimulant, then the normalization is carried out according to the Formula 9, if the indicator of the injection is negative (is a destimulator), then the normalization is based on the Formula 10.

$$x_{ij} = w_j \cdot \frac{a_j^{max} - a_{ij}}{a_j^{max} - a_j^{min}}, \tag{9}$$

$$x_{ij} = w_j \cdot \frac{a_{ij} - a_j^{min}}{a_j^{max} - a_j^{min}}, \tag{10}$$

where x_{ij} – normalized value of the *j*-indicator of cybersecurity for the *i*- country ($i = 1 \div m; j = 1 \div n$);

w_j - the weight of each *j*-indicator of cybersecurity, which reflects its importance for the overall ranking of the country, with $\sum_{j=1}^{n} w_j = 1$;

a_{ij} – the actual value of the *j*- indicator of cybersecurity for the *i*- country;

a_j^{max} - the maximum value of the *j*- indicator of cybersecurity;

a_j^{min} – the minimum value of the *j*- indicator of cybersecurity.

Since all cybersecurity indicators are stimulators, we use Formula 9 to normalize them. We use the approach to determining weights similarly to that used in the TOPSIS method.

At the third stage, we calculate the weighted and normalized distance of Manhattan (S_i) by Formula 11, as well as the weighted and normalized distance of Chebyshev (R_i) by Formula 12.

$$S_i = \sum_{j=1}^{n} x_{ij}, \tag{11}$$

$$R_i = \max_i x_{ij}. \tag{12}$$

The fourth stage calculates the estimate of the distance for the i-th country to the ideal solution, the optimal combination of cybersecurity indicators (Formula 13):

$$Q_i = v \cdot \frac{S_i - S^-}{S^+ - S^-} + (1 - v) \cdot \frac{R_i - R^-}{R^+ - R^-}, \tag{13}$$

where Q_i – estimate the distance for the *i*- country to the ideal solution, the value of which is in the range from 0 to 1. The closer it is to 0, the closer the distance for the *i*-country to the ideal solution. If the estimate is close to 1, then the parameters of the country deviate significantly from the ideal solution;

S^-, S^+ – calculated by Formula 14:

$$S^- = \min_i S_i,\ S^+ = \max_i S_i\ ; \tag{14}$$

R^-, R^+ – calculated by Formula 15:

$$R^- = \min_i R_i,\ R^+ = \max_i R_i \tag{15}$$

v – this is the weight of the strategy of most attributes or group utility, the value of which is in the range from 0 to 1. The greatest preference is given to the value of 0.5, which shows a balanced decision-making. If it is 1, then it is a strategy to maximize group utility, if 0, then a strategy to minimize individual compassion, ie there is a minimum value of the criterion for each alternative among the maximum individual deviations from the ideal value.

At the fifth stage, ranking is performed for the obtained scores in order to determine the rating of the country similar to the ranking process described in the TOPSIS method. The third method used in the study is the Multi-attribute Attitude Model (MAAM), which is based on the Fishbein Model proposed in 1963 (Miller, 1975). Its essence is to determine the attitude of consumers to a particular product depending on the estimates of its attributes. According to the conditions of this study, cybersecurity indicators will be assessed for each country in order to identify the weakest and strongest countries in terms of the conditions created by them to ensure the appropriate level of security. The method is very simple to implement and involves the following steps.

The first stage is carried out in the same way as by the TOPSIS and VIKOR methods.

The second stage determines the assessment of the overall level of cybersecurity using the Formula 16:

$$Q_i = \sum_{j=1}^{n} w_j \cdot a_{ij}, \tag{16}$$

where Q_i – assessment of the overall level of cybersecurity for the i-country;

w_j – the weight of each j- cybersecurity indicator, which reflects its importance ($\sum_{j=1}^{n} w_j = 1$);

a_{ij} – the actual value of the j-cybersecurity indicator for the i- country.

The third stage is devoted to the calculation of the rating for the i-th country, which is carried out similarly to the methods TOPSIS and VIKOR.

3. Results and Discussions

The calculations were performed using Microsoft Office Excel. As a result, country ratings were obtained according to the level of cybersecurity, which were obtained by the three methods presented in section 3.2. A fragment of the obtained results is presented in table 1. The calculation by the VIKOR method was based on the weight of group utility 1 and 0.5. At v = 0, the rating results were inadequate.

Table 1. The results of calculations of country ratings by methodsTOPSIS, MAAM, VIKOR (fragment)

№	Country	Real Rank	TOPSIS	MAAM	VIKOR	
					v=1	v=0.5
1	Afghanistan	131	134	130.5	133.5	135
2	Albania	68	71	70.5	67	90
3	Algeria	122	122	122	124	128.5
4	Angola	144	144	148.5	145.5	146
5	Antigua and Barbuda	136	141	141	133.5	135
6	Argentina	55	52	57	54.5	49
7	Armenia	91	84	81	89	84
8	Australia	36	37	37	35.5	64
9	Austria	23	24	19.5	23	20
10	Azerbaijan	80	79	79	82	79
11	Bahamas	103	105	101	102	104.5
…	…	…	…	…	…	…
149	Ukraine	29	34	24	28.5	27
150	United Arab Emirates	71	68	62	70.5	57
151	United Kingdom	14	11	12	14	11
152	United States	27	20	30.5	28.5	61
153	Uruguay	56	55	56	54.5	62
154	Uzbekistan	89	85	88	89	99.5
155	Vanuatu	138	142	142	140	141
156	Venezuela	85	82	77	85	81.5
157	Vietnam	81	73	89	80	96
158	Yemen	148	147	147	148	148
159	Zambia	66	66	67	67	71
160	Zimbabwe	118	119	115	119	112

Source: independent development by authors.

To obtain an adequate assessment, the obtained ratings were compared with the actual value of the rating generated by the National Cybersecurity Index, the value of which is given in Table 1. For analysis, the difference between the actual rating value and the calculated one was found. Figure 1 shows the difference obtained by comparing the rating method TOPSIS and real.

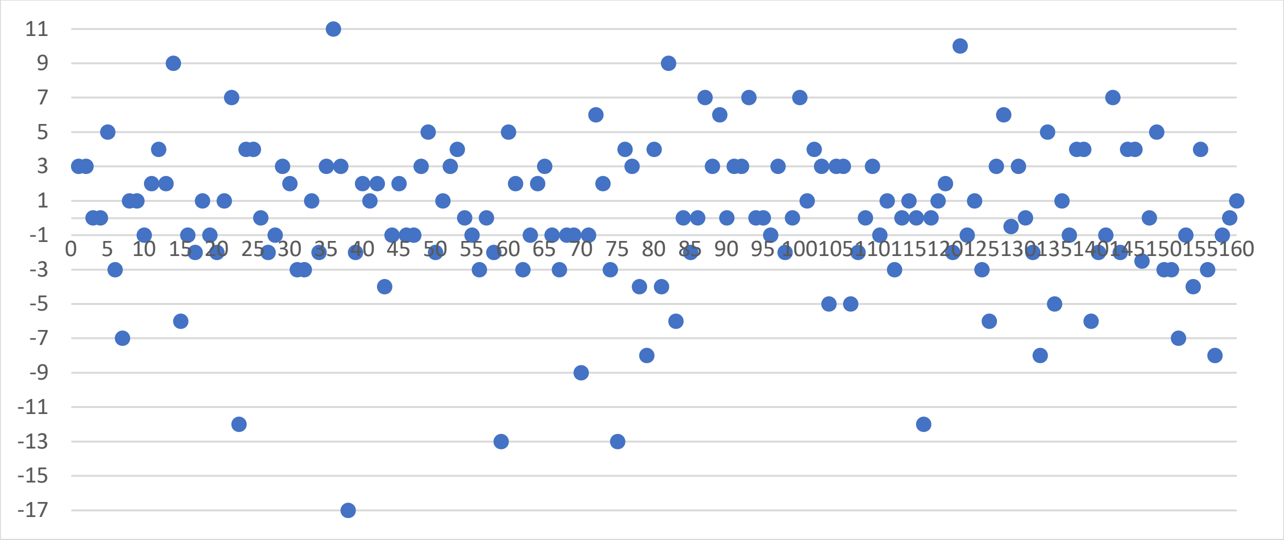

Figure 1. The difference obtained by comparing the rating by the TOPSIS method and the actual value

Source: independent development by authors.

Figure 1 shows that the deviation between the actual value and calculated by the TOPSIS method is from -17 to 11 positions, which indicates a significant variance in values. Only for 18 countries the ratings coincided, which is only 11.25% of the total number of countries. Since the approach to determining the actual rating does not take into account many aspects, such as the importance of cybersecurity indicators, estimating the deviation of values for the country on various indicators, determining the best or worst alternative, we can say that the TOPSIS rating results should be used from the standpoint strengths and weaknesses in the country's cybersecurity. To this end, a petal diagram is constructed, which allows such an analysis (Figure 2).

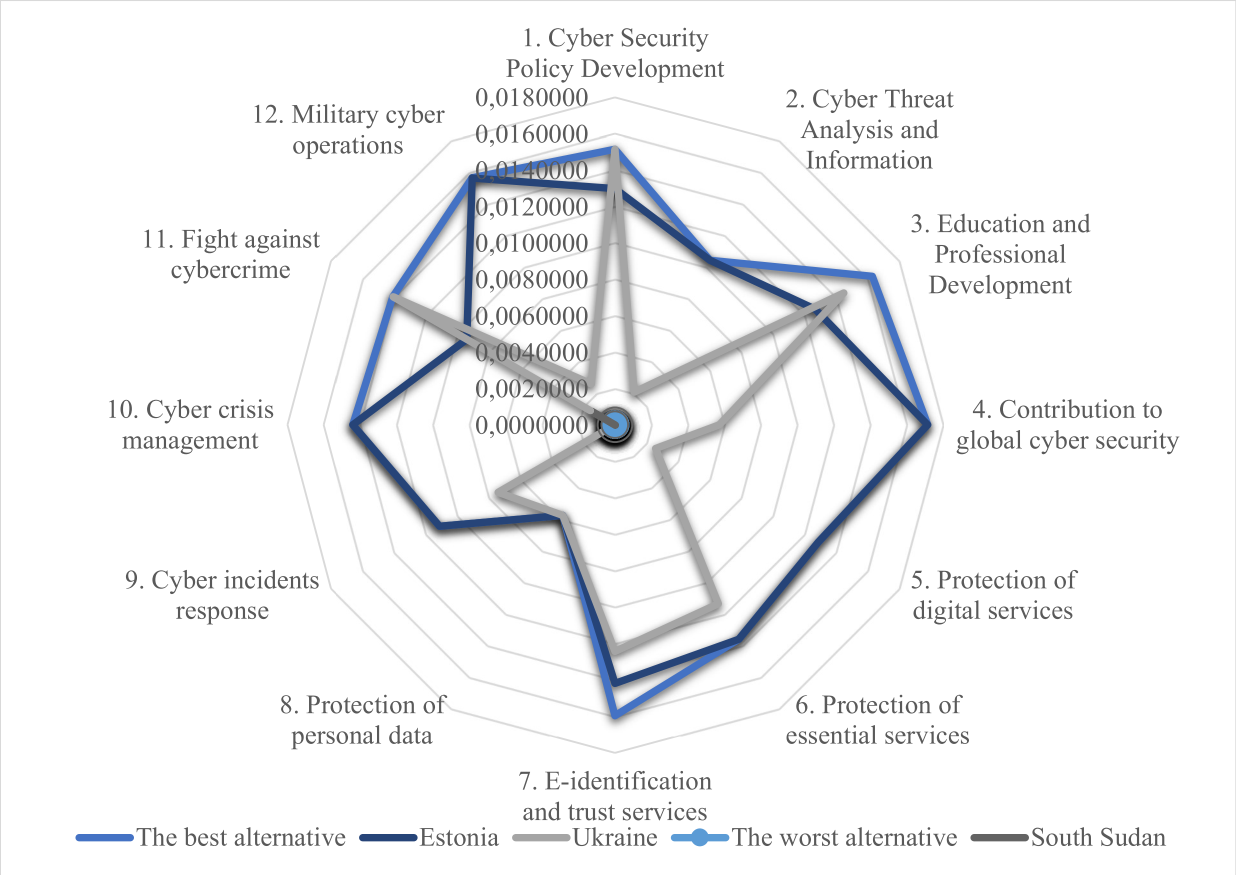

Figure 2. Diagram of alternative solutions for countries

Source: independent development by authors.

Figure 2 shows the best (positive) alternative, the worst (negative) alternative, the alternative solution for

Estonia, which ranks 1st in the ranking, the alternative for Ukraine - countries with a medium rating, the solution for South Sudan - countries that ranks last in the ranking. Since all values of the negative alternative are 0, it is visually displayed as a dot on the graph.

Analyzing the indicators for Estonia, it can be seen that this country should pay more attention to the development of Cyber Security Policy, Education and Professional Development, E-identification and trust services and Fight against cybercrime, as their values deviate from the best (positive) alternative. This indicates the existence of certain problems that require improvement of the legal framework, the introduction of new specialties related to information protection and cybersecurity, modernization of technologies in the field of electronic identification, development of more effective organizations aimed at combating cybercrime.

The results for Ukraine represent a significant contrast, as some indicators correspond to or approach the best alternative, and some others go to the worst values. That is, there are problems related to Cyber Threat Analysis and Information, Contribution to global cyber security, Protection of digital services, Protection of essential services, E-identification and trust services, Cyber incidents response, Cyber crisis management, Military cyber operations. Moreover, the Cyber crisis management indicator is generally 0, which indicates the lack of appropriate cyber security management plans, cyber crises at the national level, prompt support for volunteers during the cyber crisis, participation in international exercises on cyber security.

As for the results for South Sudan, in fact, this country does not provide cybersecurity for its citizens, businesses and the state as a whole. This is due to the history of the formation of the state and the constant military conflicts in the middle. Accordingly, today the problem of cybersecurity is not a priority for this country.

The difference obtained by comparing the actual rating of the country and the rating by the VIKOR method is shown in Figures 3 and 4. Thus, Figure 3 shows a scatter of values in the range from -3 to 3, which indicates the similarity of the results of the estimated rating to actual. 40 countries have estimates similar to those of the actual rating, which is 25% of the total. Since the value of the group utility weight v = 1 was used for the calculations when it is maximized, these results indicate a positive view of the total rating estimates for the country. The results of the calculations by the balanced approach, when v = 0.5, are presented in Figure 4, which shows the difference between the estimates with a range from -30.5 to +38. The number of countries with similar estimates is 10, which is 6.25%.

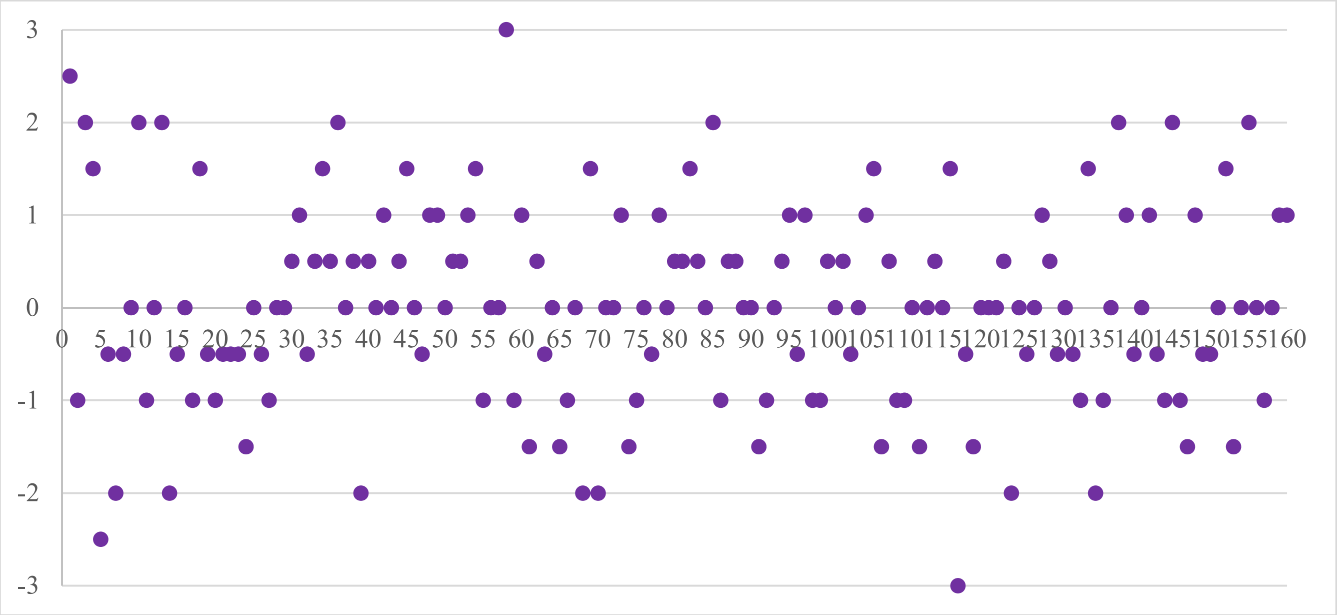

Figure 3. The difference obtained by comparing the raking by the VIKOR method and the actual value (v = 1)

Source: independent development by authors.

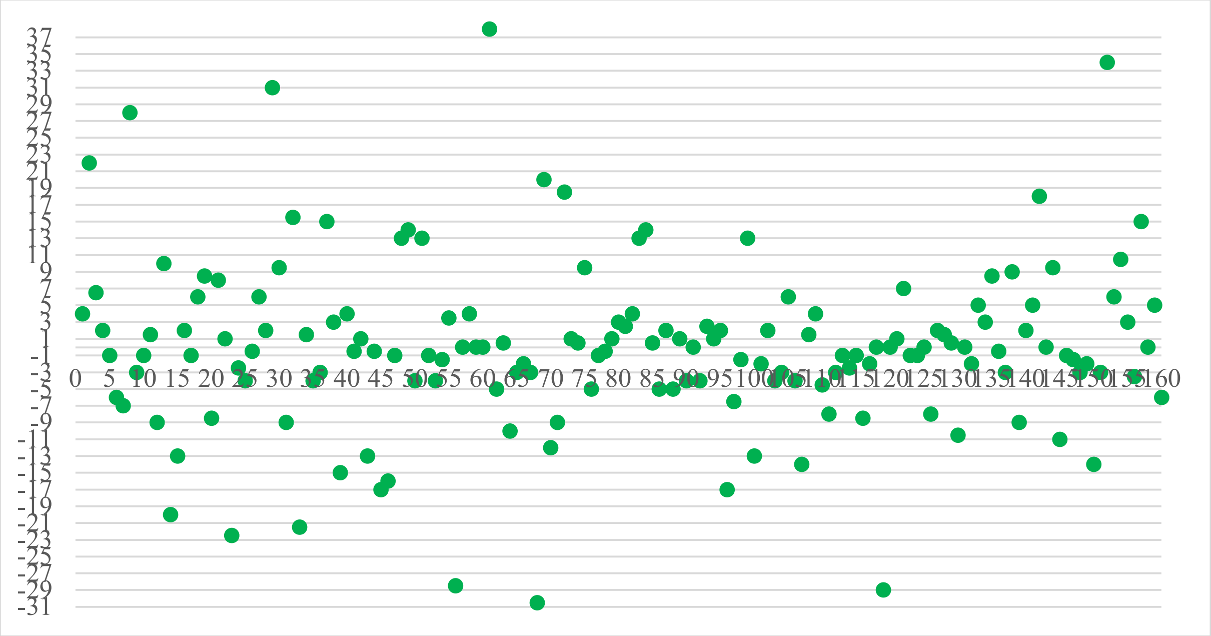

Figure 4. The difference obtained by comparing the rating by the VIKOR method and the actual value (v = 0.5)

Source: independent development by authors.

VIKOR rating, provided that v = 0.5, is appropriate in case of finding a compromise under the condition of using conflicting criteria. In the case of a study, it would be appropriate to use this method if cybersecurity indicators would have opposite values or have the opposite effect on the formation of the overall assessment.

Regarding the comparison of the rating calculated by the MAAM method with the actual rating, the obtained differences are presented in Figure 5.

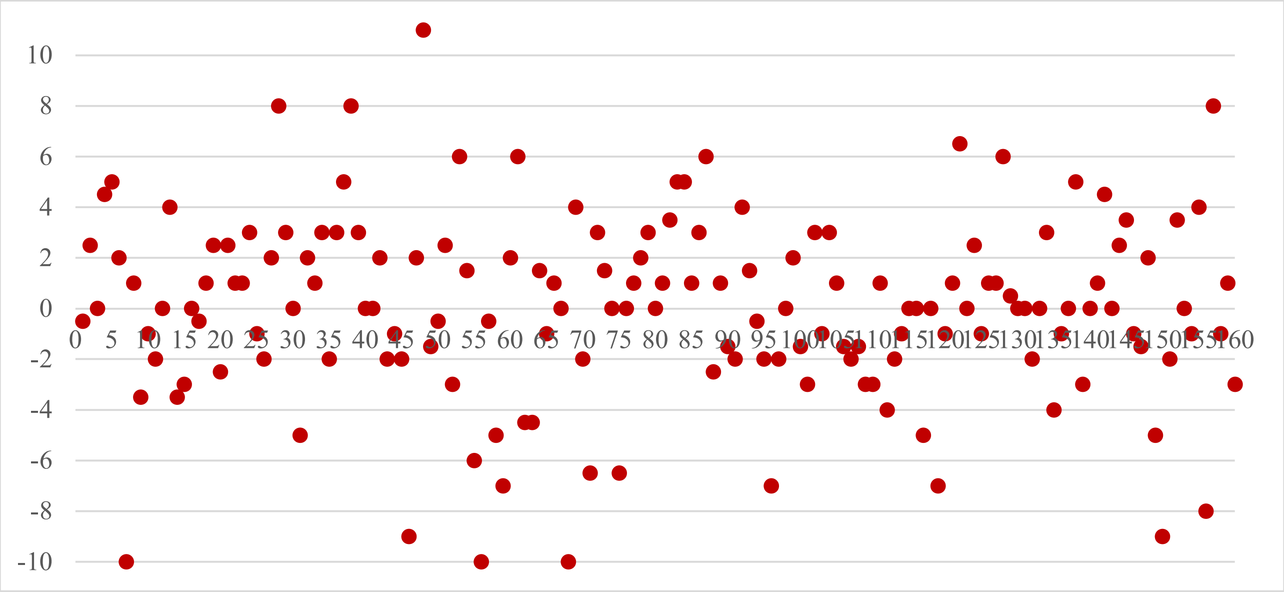

Figure 5. The difference obtained by comparing the rating by the MAAM method and the actual value

Source: independent development by authors

The comparison results in Figure 5 show that the difference between the estimates ranges from -10 to +11, ie the results are the same for 22 countries, which is approximately 13.75%. Also, these discrepancies are close to those obtained by comparing the actual rating and TOPSIS score. But this method does not involve the use of data normalization, which makes it unsuitable for use in cases where the criteria have different dimensions.

Figure 6 compares the ratings obtained for the countries with the lowest score (South Sudan), the highest score (Czech Republic and Estonia) and the moderate score (Ukraine).

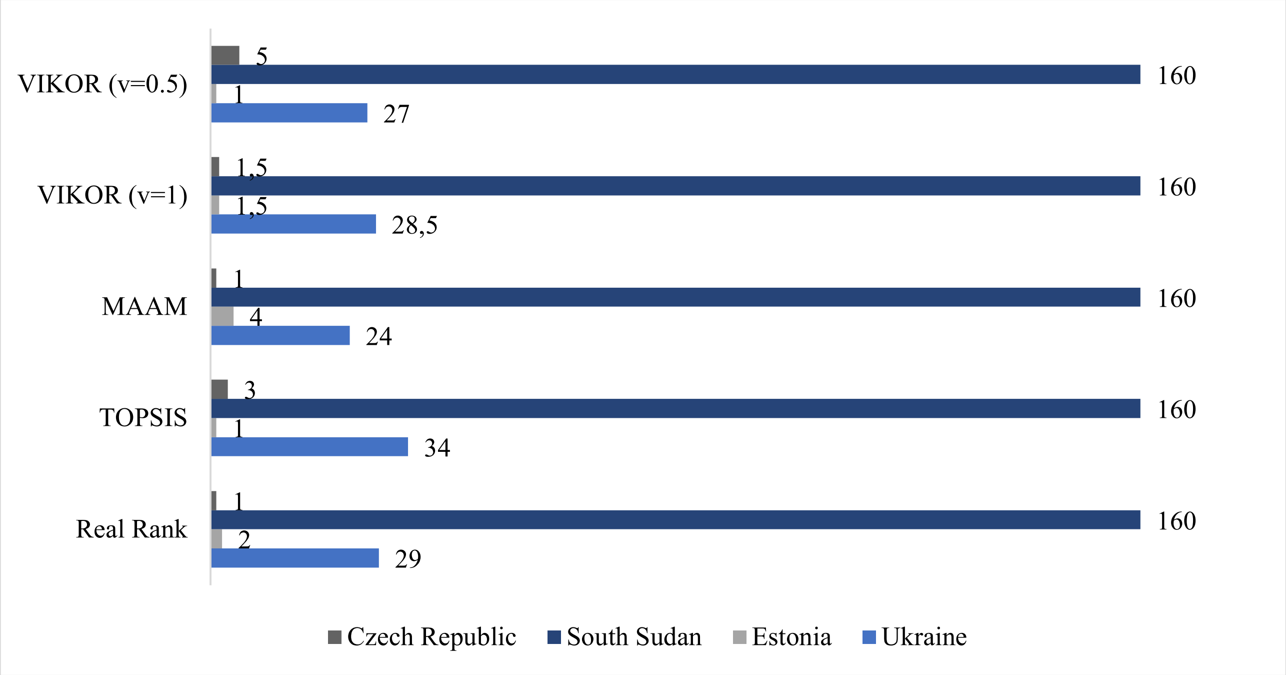

Figure 6. Comparison of rating results

Source: independent development by authors.

The countries with the best and worst indicators were selected for comparison. Thus, in the case of the Southern Courts, the same rating was obtained by all methods, which also coincides with the actual rating. For Ukraine, the results differ significantly, with the TOPSIS method assessing the country more critically, and using other methods receiving scores higher than the real rating. As for Estonia and the Czech Republic, they are leaders in different methods, with their scores ranging from 1 to 5 for the Czech Republic and from 1 to 4 for Estonia. It can be concluded that depending on the rating strategy, you can choose any of the above methods, but in the case of uneven fluctuations in the values of the criteria, their results will be radically different.

We test the effectiveness of the methods used by calculating the Spearman rank correlation coefficient according to formula 17, the results of which are shown in Table 2:

$$r = 1 - 6 \cdot \frac{\Sigma\left(d_x - d_y\right)^2}{n^3 - n}, \tag{17}$$

where r – Spearman's rank correlation coefficient;

n – number of observations;

d_x and d_y – pairs of comparable values of ranks.

Table 2. The value of Spearman's rank correlation coefficient

	Real rating	TOPSIS	MAAM	VIKOR (v=1.0)	VIKOR(v=0.5)
Real rating	1	0.9956	0.9969	0.9997	0.9759
TOPSIS	–	1	0.9940	0.9958	0.9723
MAAM	–	–	1	0.9971	0.9817
VIKOR (v=1.0)	–	–	–	1	0.9764
VIKOR(v=0.5)	–	–	–	–	1

Source: independent development by authors.

The obtained values of the correlation coefficient approach 1, which indicates the high efficiency of the obtained ranking results. But the VIKOR method (v = 0.5) gives lower efficiency results compared to other methods. Other methods have fairly equivalent estimates, which indicates a high level of confidence in the data obtained.

Conclusion

The issue of determining the ranking of countries by their level of cybersecurity is quite relevant, as it helps to obtain an adequate assessment of the country in terms of its ability to withstand cyber threats. The use of multi-attribute decision-making methods allows to solve several problems related to the dimensionality of data, determination of weights of indicators, taking into account the diversity of values of indicators and their fundamental differences. That is why the use of such methods can be an alternative in the process of determining ratings in comparison with traditional calculation methods, which are characterized by these shortcomings.

The methods of TOPSIS, VIKOR and MAAM are implemented in the work, which were used to determine the rating of countries based on estimates of indicators that characterize certain aspects of cybersecurity. As a result, the IAOM ratings are about 25% similar to the real country ratings. This indicates the low capabilities of this method, as it also has several disadvantages, as well as the assessment of the real rating. But the main advantage of this method is a simple calculation algorithm. The TOPSIS and VIKOR methods showed the best results, although VIKOR (v = 0.5) showed lower efficiency compared to other methods, as evidenced by the obtained results of Spearman's rank correlation coefficient. The estimates obtained are balanced, which indicates good opportunities for the application of this method in the process of determining the ranking of countries in terms of their level of cybersecurity. VIKOR (v = 1.0) also showed differences from real rating estimates, although the differences are the smallest compared to other methods. Because the choice of such a value of weight indicates the maximization of the group usefulness of indicators, which is appropriate in the case of choosing alternatives. But in the case of rating only, this factor can significantly affect the results, which is unacceptable for the assessment of an individual country.

The TOPSIS method is the most acceptable for ranking countries by level of cybersecurity, as it has high efficiency indicators, eliminates the listed shortcomings of real assessment methods, allows to identify alternative strategies in contrast to other methods that can also be used to analyze individual indicators. Therefore, we believe that in terms of solving the research problem, this method will not only provide effective rating assessments, but will help identify critical indicators for each country, identify countries with ideal alternatives, which will help study their experience in developing cybersecurity strategies.

In the process of comparing the estimates calculated by different methods, it was found that the countries of Estonia and the Czech Republic have the highest ratings and the value of their indicators is closest to ideal. That is, it is advisable to pay attention to their practice in forming a cybersecurity strategy, especially in terms of those indicators that for each individual country deviate significantly from the ideal and are critical. The country with the lowest rating, which was confirmed by calculations by all methods, is South Sudan. As it has problems of political, military, socio-economic nature, this confirms the lack of priority to ensure its cyber defense.

In the future, it would be useful to explore the specific features of developing a cybersecurity strategy for individual groups of countries, which will identify problems that are common to most of them and contribute to the development of universal solutions.

Acknowledgment

This work is carried out within the taxpayer-funded researches: No. 0118U003574 "Cybersecurity in the banking frauds enforcement: protection of financial service consumers and the financial and economic security growth in Ukraine", No. 0118U003574 "Modeling and forecasting socio-economic and political road reform map in Ukraine for the transition to the model of modern business", "Quadrocentric recrusive model of Ukrainian unshadow economy to increase its macroeconomic stability" and "Optimization and automation of financial monitoring processes to increase information security of Ukraine".

Funding: Economic Cybernetics Department of Sumy State University.

Author Contributions: conceptualization, Hanna Yarovenko; data curation, Olha Kuzmenko; formal analysis, Hanna Yarovenko; funding acquisition, Olha Kuzmenko; investigation, Hanna Yarovenko; methodology, Hanna Yarovenko; project administration, Mario Stumpo; resources, Mario Stumpo; software, Hanna Yarovenko; supervision, Olha Kuzmenko; validation, Mario Stumpo; visualization, Hanna Yarovenko; writing – original draft, Hanna Yarovenko; writing – review & editing, Hanna Yarovenko.

References

1. Ghernouti-Hélie, S. (2010, February). A national strategy for an effective cybersecurity approach and culture. In *5th International Conference on Availability, Reliability, and Security, ARES 2010 (Krakow; Poland; 15 February 2010 through 18 February 2010)*, 370-373. IEEE. Retrieved from: https://www.semanticscholar.org/paper/A-National-Strategy-for-an-Effective-Cybersecurity-Ghernouti-H%C3%A9lie/29283b90ba70442be97ed97d1083529f30e70603

2. Galinec, D., Moznik, D. and Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika*, 58(3), 273-286. DOI: 10.1080/00051144.2017.1407022

3. Teoh, C.S. and Mahmood, A.K. (2017). National cyber security strategies for digital economy. *Journal of Theoretical and Applied Information Technology*, 9(13), 6510-6522. Retrieved from: https://www.researchgate.net/publication/322150967_National_cyber_security_strategies_for_digital_economy

4. Kshetri, N. and Murugesan, S. (2013). EU and US cybersecurity strategies and their impact on businesses and consumers. *Computer*, 46(10), 84-88. DOI: 10.1109/MC.2013.350.

5. Kostyuk, N. (2014). International and domestic challenges to comprehensive national cybersecurity: A case study of the Czech Republic. *Journal of Strategic Security, 7*(1), 68-82. DOI: 10.5038/1944-0472.7.1.6.

6. Štitilis, D., Pakutinskas, P. and Malinauskaite, I. (2017). EU and NATO cybersecurity strategies and national cyber security strategies: A comparative analysis. *Security Journal*, *30*(4), 1151-1168. DOI: 10.1057/s41284-016-0083-9.

7. Jacobs, P., Von Solms, B. and Grobler, M. (2017). Towards a national cybersecurity capability development model. In *16th European Conference on Cyber Warfare and Security, ECCWS 2017 (Dublin; Ireland)*, 582-592. Retrieved from: http://researchspace.csir.co.za/dspace/handle/10204/9458

8. Kolini, F. and Janczewski, L. (2017). Clustering and topic modelling: A new approach for analysis of national cybersecurity strategies. In *Pacific Asia Conference on Information Systems (PACIS)*. Association For Information Systems, 2017. Retrieved from: https://core.ac.uk/download/pdf/301372894.pdf

9. Fenton, N. and Neil, M. (2012). Risk assessment and decision analysis with bayesian networks. In *Risk Assessment and Decision Analysis with Bayesian Networks*, 1-494. DOI: 10.1201/b21982). CRC Press.

10. Noel, S., Harley, E., Tam, K.H., Limiero, M. and Share, M. (2016). CyGraph: Graph-Based Analytics and Visualization for Cybersecurity. *Handbook of Statistics*, 35, 117-167. DOI: 10.1016/bs.host.2016.07.001.

11. Zhang, R., Xue, R. and Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys*, 52(3), 1-34. Retrieved from: https://arxiv.org/pdf/1903.07602

12. Yarovenko, H.M. (2004). Aspekty avtomatyzatsii finansovoho kontroliu pidpryiemstv [Aspects of automation of financial control of enterprises]. *Bulletin of the Ukrainian Academy of Banking, 2*(17), 89-96. URL: https://essuir.sumdu.edu.ua/handle/123456789/54128. [in Ukrainian]

13. Akram, S.M., Al-Kenani, A.N. and Alcantud, J.C.R. (2019). Group Decision-Making Based on the VIKOR Method with Trapezoidal Bipolar Fuzzy Information. *Symmetry*, 11, 1313. DOI: 10.3390/sym11101313.

14. Ghaleb, A. M., Kaid, H., Alsamhan, A., Mian, S. H. and Hidri, L. (2020). Assessment and Comparison of Various MCDM Approaches in the Selection of Manufacturing Process. *Advances in Materials Science and Engineering*. DOI: 10.1155/2020/4039253.

15. Mardani, A., Zavadskas, E.K., Govindan, K., Amat Senin, A. and Jusoh, A. . (2016). VIKOR technique: A systematic review of the state of the art literature on methodologies and applications. *Sustainability,* 8(1), 37. DOI: 10.3390/su8010037.

16. Suniantara, I. K. P. and Putra, I. G. E. W. (2019). Comparison of VIKOR and TOPSIS Methods in Multiresponse Taguchi Optimization. *Journal of Education Research and Evaluation*, 2(3), 106-113. URL: https://ejournal.undiksha.ac.id/index.php/JERE.

17. Chatterjeea, P. and Chakraborty, S. (2016). A comparative analysis of VIKOR method and its variants.

Decision Science Letters, 5, 469–486. DOI: 10.5267/j.dsl.2016.5.004.

18. e-Governance Academy Foundation. (2020). National Cyber Security Index. Retrieved from NCSI: https://ncsi.ega.ee/ncsi-index/

19. Hwang, C.L. and Yoon, K. (1981). Multiple Attribute Decision Making: Methods and Applications. New York: Springer-Verlag. DOI: 10.1007/978-3-642-48318-9.

20. Opricovic, S. T. G.-H. (2004.). The Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS. *European Journal of Operational Research*, *156*(2). 445–455. Retrieved from: https://www.academia.edu/3288444/Compromise_solution_by_MCDM_methods_A_comparative_analysis_of_VIKOR_and_TOPSIS

21. Miller, K.E. (1975). A Situational Multi-Attribute Attitude Model. *Advances in Consumer Research*, 2, 455-464.