SocioEconomic Challenges, Volume 4, Issue 3, 2020
ISSN (print) – 2520-6621, ISSN (online) – 2520-6214

DEA-Analysis Of The Effectiveness Of The Country's Information Security System

https://doi.org/10.21272/sec.4(3).142-153.2020.

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

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

Mario Stumpo, ORCID: https://orcid.org/0000-0001-5132-6041

Founder & Director at Bmybit LTD, London, United Kingdom

Abstract

The consequences of the fourth industrial revolution caused an increase in the level of computerization and digitalization of society, which led to problems related to the protection of information of individual users, companies and the state as a whole. The aim of this paper is to analyze the effectiveness of the information security system of countries in terms of its ability to counter information threats. Two groups of input indicators were used for this purpose. The first group was formed by 12 indicators of the country's world development, which were selected from the World Bank database and based on the results of correlation analysis. The second group includes 5 information technology indicators that characterize certain areas of information security: information technology development, digitalization of the country, countries' commitment to cybersecurity, readiness to counter cyber threats and use the latest information and communication technologies. The country's information security threat index is used as a starting point. Data from 159 countries of the world for 2018 were taken for the analysis, as for this number of countries and period there is a complete set of data on selected indicators. Country data were considered based on clusters, which allowed the use of 7 groups. The analysis was performed using the analytical tool Frontier Analyst. The study built CRR and BCC models, among which CRR was preferred, which allowed a more critical assessment of the potential of countries. The paper analyzes the structural effectiveness of socio-economic development indicators and information security indicators of countries, considering the current level of the information security threat index. As a result, the following were identified: an increase in government security spending for zero-cluster countries; the need to transform the information technology component for the countries of the first and second clusters; increasing personal protection, strengthening corruption control and legal regulation for third cluster countries; the need for economic growth and higher social standards for the fourth, fifth and sixth clusters. The obtained models allowed us to estimate the maximum level of growth of the information security threat index with the available resource potential of the country. As a result, it was found that the largest increase in the information security threat index is possible due to the existing potential of the countries of the zero and fifth clusters, which will increase the effectiveness of their response to information threats.

Keywords: BBC-model, CCR-model, Data Envelopment Analysis, socio-economic development, information, threat, security.

JEL Classification: C10, C43, O30.

Cite as: Yarovenko, H., Kuzmenko, O., Stumpo, M. (2020). Data Envelopment Analysis of Efficiency of Country Information Security System. *SocioEconomic Challenges*, *4*(3), 142-153. https://doi.org/10.21272/sec.4(3).142-153.2020.

1. Introduction

The consequences of the fourth industrial revolution "Industry 4.0" led to the emergence of the latest cyberphysical systems and digital technologies, which have influenced the development of many areas of the economy. As a result, "smart" businesses have emerged, most trading operations have been transferred online to web platforms, and the use of mobile and Internet banking has supplanted cash transactions. The population also prefers to use the Internet, software, and mobile applications in everyday life, which facilitates many transactions, from fares on public transport to banking transactions. On the other hand, the rapid computerization, digitization, and informatization of many processes have contributed to the rise of cybercrime in society. This manifests itself in hacking attacks, cyber-fraud to steal personal and confidential information of a person or company, creating and spreading viruses to damage user data, conducting information wars aimed at shaking society, which can lead to economic and social crisis, and so on. That is, there is a need to create a set of measures to combat such threats, which is manifested in the formation of information security, which aims to ensure the integrity, confidentiality and protection of information to prevent its unauthorized use, theft, distortion, alteration, damage and destruction.

This problem is relevant for the state, as the impact of information threats at the level of individual businesses on the economy can be enormous. Thus, the leakage of information leads to an average loss of the company in the amount of 3.86 million dollars annually (Ponemon Institute, 2019). Companies that do not have appropriate response teams spend up to $ 5.29 million to overcome the consequences associated with the loss of information, and the losses of economic entities that carry out appropriate regular measures to identify information losses amount to $ 2 million lower. It is also projected to increase the losses of companies as a result of violation of their information security from 3 trillion dollars in 2018 to 5 trillion dollars in 2024 (Morrow and Crabtree, 2019), which speaks only of the increasing problem of data protection in the future. That is why there is a need for a comprehensive analysis of the effectiveness of the system of measures of the state to identify opportunities to overcome the consequences of information threats. Its implementation should also include an analysis of the country's existing potential, which is characterized by the level of economic, social, and political development of the country. It is also necessary to have an idea of the prospects for the existence of resources reserve of that will provide ways to increase opportunities to combat information threats and ensure a stable level of information security.

2. Literature Review

A wide range of scientists deals with current issues related to the information security of the state and business entities. There are studies that try to address the issue of improving the efficiency of the country's information security system through its further reform (Loshytskyi et al., 2020). Frolova et al. (2018) propose in the applied and legal aspect to develop measures to ensure better management of the information security system at the micro and macro levels. Deane et al. (2019) explore the areas of creation and development of information security management program, which provide for an increase in investment in this area. Kosevich (2020) proposes options for developing existing cybersecurity strategies, which also include the creation of special services and organizations that will be responsible for the implementation of protection in the country.

A number of scientists analyze the effectiveness of the information security system to counter information threats. This aspect is the subject of a study by Sorokivska (2015), which examines the impact of information wars on information and economic security of companies. Other scientists suggest the use of specialized indices that will analyze the current state of information security. Thus, Jazri et al. (2018) propose to develop an index of recovery of the cybersecurity system, which would allow the analysis of its possible components that require additional funding and implementation of software and hardware and organizational measures. Yunis and Koong (2015) developed a conceptual model for creating a comprehensive national cybersecurity index that considers various factors that affect the level of cybersecurity. We can also highlight the work of Tolubko et al. (2018), which was devoted to the development of an integrated criterion for the effectiveness of information protection formation in the presence of risks of information threats.

Economic and mathematical methods are quite popular, which allow the analysis of various aspects of activity. Fedotova et al. (2019) applied statistical and systematic analysis to identify the impact of threats on the level of economic and information security of enterprises. Hu et al. (2017) used methods to optimize the security of data accounting to improve the efficiency of existing information security systems. The method of

discriminatory scales for the analysis of information security risks is proposed by Chen et al. (2014). Dudykevych et al. (2019) applied multicriteria analysis to assess the effectiveness of conservative information protection systems.

Thus, the issue of information security research is quite broad, but the direction of analysis of the effectiveness of the information security system in countries in terms of its ability to counter information threats is poorly represented by scientific papers.

3. Data and Methodology

3.1. Data

Two groups of indicators were taken for the study, which characterize the level of information security of the country and the level of its development. The first group includes indicators: Global Cybersecurity Index; National Cyber Security Index; ICT Development Index; Networked Readiness Index; Digital Development Level, each of which defines only a separate area of information security of the country. Yes, the Global Cybersecurity Index is used to measure countries' commitment to cybersecurity globally. The National Cyber Security Index is used to determine a country's readiness to counter cyber threats; level of information technology development in the country – ICT Development Index; the degree of technological readiness of the country for the application of the latest information and communication technologies in various fields – Networked Readiness Index; level of digitalization of the country – Digital Development Level (e-Governance Academy Foundation, 2020). The second group included indicators of economic, social and political development of the country, which were analyzed for the presence of a correlation with the indicators that characterize the level of information security of the country. As a result, 12 indicators with a correlation level greater than 0.5 or -0.5 were selected. That is, the second group was formed by: GDP per capita (current US$); Life expectancy; Wage and salaried workers, total (% of total employment); Control of Corruption: Estimate; Government Effectiveness: Estimate; Regulatory Quality: Estimate; Rule of Law: Estimate; GNI per capita, PPP (current international $); Mobile cellular subscriptions (per 100 people); Revenue, excluding grants (% of GDP); Individuals using the Internet (% of population); General government expenditure (% of GDP) (The World Bank, 2020). The input data were taken for calculations for 2018 for 159 countries, as this time period contains the most complete information on the selected indices. As the level of development and security of countries is very different, which can lead to conflicting results, clustering was carried out using self-organized Kohonen maps, which allowed to form 7 groups of countries: 0th and 1st cluster includes countries with the highest development and security, 2nd – above-average countries, 3rd – with average level of development and security, 4th – below average, 5th – low, 6th – very low (Yarovenko, 2020a). The obtained groups will allow to evaluate the effectiveness of the information security system in terms of opportunities to counter information threats in countries that have approximately the same conditions for development. These indicators formed a set of input changes for further analysis. According to the quality of the initial change, the index of the level of information security threats of countries was chosen, which can assess the level of countries in terms of opportunities to overcome the consequences of information threats to information security (Yarovenko, 2020b).

3.2. Metodology

The study was performed using the DEA method – Data Envelopment Analysis, which was proposed by A. Charnes, W. Cooper and E. Rhodes in 1978 (Charnes et al., 1978). This tool is used in many industries to evaluate the effectiveness of complex systems, which occurs by solving the optimization problem of linear programming. Its purpose is to determine the efficiency of the system based on the ratio of its outputs and inputs, it is necessary to consider the maximum output of resources at a given level of inputs, or the minimum level of resources at a given level of outputs. The use of the DEA-method will determine the effectiveness of the level of the country's information security system to counter threats, considering the country's potential, namely socio-economic and information technology. Effectiveness will be achieved when the level of threat response for an individual country cannot be increased, while the level of development and security of the country will be at the same level. Also it is possible in the case when the reduction of the level of development and security of the country leads to changes in the level of counteraction to information threats. Based on the above, it is possible to form an initial DEA-model (Charnes et al., 1978), which will be used to assess the effectiveness of the level of information security of the country (equation 1):

$$\max \theta_s = \frac{\sum_{p=1}^{z} u_{ps} y_{ps}}{\sum_{i=1}^{m} v_{is} x_{is}} \quad (1)$$

$$\begin{cases} \frac{\sum_{p=1}^{z} u_{ps} y_{pj}}{\sum_{i=1}^{m} v_{is} x_i j} \leq 1, \\ s, j = \overline{1, n}, \\ u_p, v_i \geq 0, \\ y_{p,} x_i \geq 0. \end{cases}$$

where θ is the level of efficiency of the information security system for a particular country, defined as the ratio between the weighted sum of outputs and inputs; u_p are weights of outputs that maximize the efficiency of the evaluated unit θ; v_p are weights of outputs that maximize the efficiency of the evaluated unit θ;ny$_p$ is the p-th characteristic of conditional outputs, i.e. the values of the index of the level of information security threat for each country; x_i is the i-th characteristic of conditional inputs, i.e. values of indicators of information security and indicators of development of the country.

Restrictions (equation 1) say that the ratio of output to input can not exceed 1 for each θ. Therefore, the presented fractional problem should be turned into a linear one, which greatly simplifies its further use. Accordingly, there are two types of DEA models – CCR, which was proposed by Charnes A., Cooper W. and Rhodes E. (Charnes et al., 1978) in 1978, and BCC, which was developed based on the CCR model in 1984, Banker R., Charnes A. and Cooper W. (Banker et al., 1984). Each of these models is focused on input (resources) and output (result indicators) (equations 2 – 5).

$$\max_{u,v} w_s = \sum_{p=1}^{z} u_{ps} y_{ps}$$

$$\begin{cases} \sum_{i=1}^{m} v_{is} x_{is} = 1 \\ \sum_{p=1}^{z} u_{ps} y_{pj} - \sum_{i=1}^{m} v_{is} x_{ij} \leq 0 \\ u_p, v_i \geq \gamma \end{cases} \quad (2)$$

$$\max_{u,v,k} w_s = \sum_{p=1}^{z} u_{ps} y_{ps} + k_s$$

$$\begin{cases} \sum_{i=1}^{m} v_{is} x_{is} = 1 \\ \sum_{p=1}^{z} u_{ps} y_{pj} + k_s \leq \sum_{i=1}^{m} v_{is} x_{ij} \\ u_p, v_i \geq \gamma \\ k_s - \ unconstrained \end{cases} \quad (3)$$

$$\min_{\alpha,\beta} w_s = \sum_{i=1}^{m} \beta_i x_{is}$$

$$\begin{cases} \sum_{p=1}^{z} \alpha_p y_{ps} = 1 \\ \sum_{i=1}^{m} \beta_i x_{ij} - \sum_{p=1}^{z} \alpha_p y_{pj} \geq 0 \\ \alpha_p, \beta_i \geq \gamma \end{cases} \quad (4)$$

$$\min_{\alpha,\beta,k} w_s = \sum_{i=1}^{m} \beta_i x_{is} - k_s$$

$$\begin{cases} \sum_{p=1}^{z} \alpha_p y_{ps} = 1 \\ \sum_{i=1}^{m} \beta_i x_{ij} - k_s \geq \sum_{p=1}^{z} \alpha_p y_{pj} \\ \alpha_p, \beta_i \geq \gamma \\ k_s - \ unconstrained \end{cases} \quad (5)$$

where γ is is a small positive real number that eliminates the possibility of variables becoming zero.

Models CCR (equation 2) and BCC (equation 3) are Input-oriented models, i.e. aimed at assessing the effectiveness of the distribution of development indicators in the country and their information security, which helps to identify structural inefficiencies of given indices. The CCR (equation 4) and BCC (equation 5) models are Output-oriented, i.e. they allow to assess the effectiveness of the country's information security system by determining the maximum values of the information security threat level index, given the set values of development and information security indicators.

4. Results and Discussions

Data Envelopment Analysis was performed in the analytical package "Frontier Analyst", which allows calculations based on CCR and BCC models (Banxia Software, 2020). As a demo version was used, 12 representatives were selected in each country cluster for the Data Envelopment Analysis. The minimum value of scales in the program was set based on the calculation of Total redundancy, as a share of its value in the total (Yarovenko, 2020b). When determining the minimum weights, it was taken into account that security indicators have an equivalent effect on the index of information security threats. The maximum value of the scales was set at 100%.

The zero cluster is represented by countries with the highest indicators of socio-economic development, the level of informatization and computerization. The results of evaluations of their effectiveness are presented in Figures 1-4.

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Estonia	100,0%	✓	
Israel	100,0%	✓	
New Zealand	100,0%	✓	
Netherlands	100,0%	✓	
Austria	99,9%		
Luxembourg	99,8%		
United Kingdom	99,7%		
Australia	99,5%		
Norway	99,2%		
France	99,2%		
United States	98,8%		
Belgium	98,4%		

Figure 1. Output-oriented BCC model

Source: independent development by authors.

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Israel	100,0%	✓	
Estonia	95,5%		
Belgium	91,4%		
New Zealand	91,4%		
France	90,7%		
Australia	89,8%		
United States	89,4%		
Austria	89,0%		
United Kingdom	87,4%		
Luxembourg	82,5%		
Netherlands	82,1%		
Norway	81,3%		

Figure 2. Output-oriented CCR model

Source: independent development by authors.

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Israel	100,0%	✓	
New Zealand	100,0%	✓	
Estonia	100,0%	✓	
Netherlands	100,0%	✓	
Austria	93,7%		
Belgium	92,4%		
France	90,9%		
United States	89,9%		
Australia	89,8%		
United Kingdom	87,1%		
Luxembourg	86,0%		
Norway	81,1%		

Figure 3. Input-oriented BCC model

Source: independent development by authors.

Units	Comparison 1		
Unit name	Score	Efficient	Condition
Israel	100,0%	✓	
Estonia	95,3%		
Belgium	91,1%		
New Zealand	91,1%		
France	90,5%		
Australia	89,6%		
United States	89,1%		
Austria	88,7%		
United Kingdom	87,1%		
Luxembourg	82,0%		
Netherlands	81,5%		
Norway	80,8%		

Figure 4. Input-oriented CCR model

Source: independent development by authors.

If we compare the results of obtained models (Figures 1-4), we can see that the CCR model is more restrictive than the BCC, i.e. it allowed to identify only 1 country (Israel), which has an efficiency for inputs and outputs of 100%. Accordingly, 4 countries with 100% input and output efficiency were obtained according to the BCC model – Israel, New Zealand, Estonia, Netherlands. That is, the countries Austria, Belgium, France, United States, Australia, the United Kingdom, Luxembourg and Norway, which belong to the cluster of countries with high development and security, are not able to achieve 100% efficiency of information security system according to BCC models and CCR. As for the countries of other clusters, the results of the analysis of the effectiveness of their information security system are presented in Table 1. Since the BCC model overestimates the efficiency results, Table 1 contains calculations Output-oriented and Input-oriented CCR-model.

Table 1. The effectiveness of the information security system of countries in the Output-oriented and Input-oriented CCR-model

Country	Maximize outputs	Minimize inputs	Country	Maximize outputs	Minimize inputs
Cluster 1			**Cluster 4**		
Japan	91,3%	91,0%	Kazakhstan	88,4%	88,1%
Qatar	100,0%	100,0%	Mexico	85,5%	85,0%
Spain	100,0%	100,0%	Russian Federation	73,5%	72,7%
United Arab Emirates	100,0%	100,0%	South Africa	100,0%	100,0%
Cluster 2			Turkey	90,0%	89,7%
Bulgaria	100,0%	100,0%	Ukraine	79,3%	78,7%
Chile	100,0%	100,0%	**Cluster 5**		
Czech Republic	93,6%	93,4%	Algeria	65,7%	64,8%
Greece	95,9%	95,8%	Bhutan	83,8%	83,3%
Italy	93,3%	93,1%	China	100,0%	100,0%
Latvia	92,7%	92,5%	Egypt	71,3%	70,4%
Lithuania	90,2%	89,9%	India	65,2%	64,2%
Poland	96,8%	96,7%	Indonesia	96,6%	96,5%
Romania	97,8%	97,7%	Kenya	69,5%	68,6%
Saudi Arabia	92,6%	92,4%	Panama	100,0%	100,0%
Slovakia	95,2%	95,1%	Peru	100,0%	10,0%
Slovenia	95,0%	94,9%	Tunisia	100,0%	100,0%
Cluster 3			Uzbekistan	100,0%	100,0%
Bahamas	100,0%	100,0%	Vietnam	87,7%	87,4%
Bahrain	90,9%	90,6%	**Cluster 6**		
Barbados	100,0%	100,0%	Benin	100,0%	100,0%
Brunei Darussalam	100,0%	100,0%	Cameroon	100,0%	100,0%
Korea (Republic of)	100,0%	100,0%	Ethiopia	100,0%	100,0%
Montenegro	100,0%	100,0%	Lao PDR	87,4%	87,0%
Oman	96,1%	95,9%	Malawi	100,0%	100,0%
Serbia	100,0%	100,0%	Mali	100,0%	100,0%
Cluster 4			Mauritania	100,0%	100,0%
Albania	89,2%	88,9%	Mozambique	100,0%	100,0%
Argentina	94,9%	94,8%	Myanmar	100,0%	100,0%
Armenia	100,0%	100,0%	Nigeria	93,1%	92,9%
Brazil	89,6%	89,3%	Vanuatu	100,0%	100,0%
Colombia	95,4%	95,3%	Zimbabwe	94,1%	93,9%
Georgia	100,0%	100,0%			

Source: independent development by authors.

Analyzing the results presented in Table 1, authors can say that a number of countries have achieved the effectiveness of the information security system in terms of combating information threats. These include countries of the 1st cluster – Qatar, Spain, United Arab Emirates; countries of the 2nd cluster – Bulgaria, Chile; countries of the 3rd cluster – Bahamas, Barbados, Brunei Darussalam, the Republic of Korea, Montenegro, Serbia; countries of the 4th cluster – Armenia, Georgia, South Africa; countries of the 5th cluster – China, Panama, Peru, Tunisia, Uzbekistan; countries of the 6th cluster – Benin, Cameroon, Ethiopia, Malawi, Mali, Mauritania, Mozambique, Myanmar, Vanuatu. The results for other countries suggest that they should pay attention to those areas that contribute to efficiency to achieve 100% value within the cluster. This may be due to the fact that a number of input resources need to improve or increase the efficiency of the level of information security, possibly due to the formation of reserves of individual indicators. Thus, authors analyze the structural efficiency of the input indicators for the countries of the zero cluster, obtained as a result of the analysis of the Input-oriented CCR-model (Figure 5). Figure 5 shows the structural effectiveness of indicators of socio-economic development in countries and the level of aspects of their security. Thus, Life expectancy (0.63%), Mobile cellular subscriptions (2.5%) and General government expenditure (7.47%) need to be improved to ensure the effectiveness of the information security system at the actual level. Since Life expectancy is an uncontrolled input index, only the other two indicators should be a country priority for development. That is, the country's development strategy should consider such areas as security and protection expenditures provided by public administration. Accordingly, their increase will improve the efficiency of government agencies to ensure the protection of information and security of operations. It should also be borne in mind that the growth of Mobile cellular subscriptions will help to increase personal protection and the development of mobile security systems based on the use of modern cellular technologies. As for other input parameters, their values indicate that countries

have a certain reserve, the use of which can increase the level of protection in the country. Authors will analyze the potential for improving the efficiency of the information security system of zero cluster countries, provided that the index of the level of information security threat is maximized. The results of the Output-oriented CCR-model are presented in Figure 6.

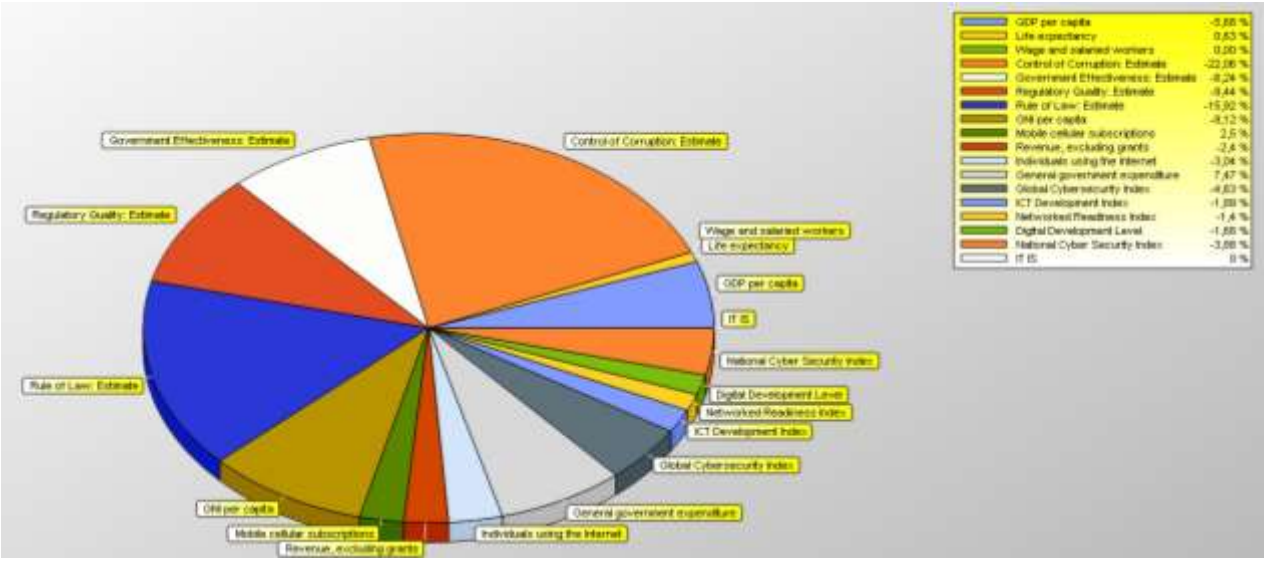

Figure 5. The potential for improving the efficiency of the information security system of the zero cluster countries (Input-oriented CCR-model)

Source: independent development by authors.

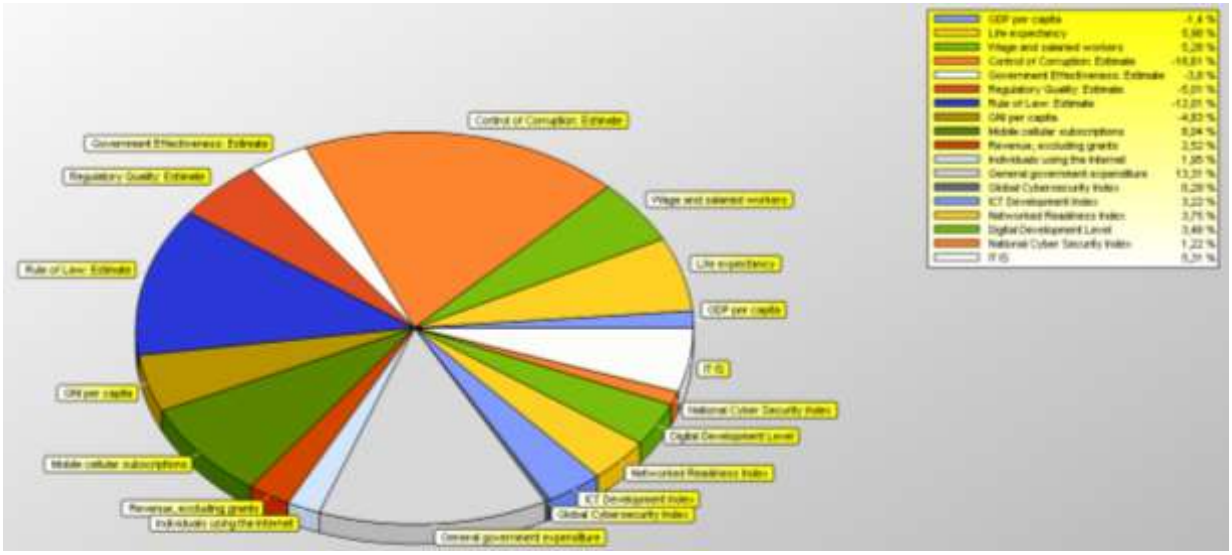

Figure 6. Potential to improve the efficiency of the information security system of zero cluster countries (Output-oriented CCR-model)

Source: independent development by authors.

The results of the Output-oriented CCR-model (see Figure 6) show that the maximum growth of the information security threat level index is possible by 5.31%, which can be ensured due to the existence of potential reserves in terms of GDP per capita (-1,4%); Control of Corruption: Estimate (-18.61%); Government Effectiveness: Estimate (-3.8%); Regulatory Quality: Estimate (-5.01%); Rule of Law: Estimate (-12.01%); GNI per capita (-4.83%). That is, zero cluster countries have significant economic potential, effective government, high-quality legislative and regulatory bodies, which can increase the level of information security of the country. On the other hand, to ensure the maximum level of opportunities for the country to overcome the consequences of information threats, a number of measures should be developed to

increase such indicators as Wage and salaried workers (5.28%); Mobile cellular subscriptions (8.04%); Revenue, excluding grants (2.52%); Individuals using the Internet (1.95%); General government expenditure (13.31%); Global Cybersecurity Index (0.29%); National Cyber Security Index (1.22%); ICT Development Index (3.22%); Networked Readiness Index (3.75%); Digital Development Level (3.46%).

As for the potential of other clusters, Figure 7 presents its results based on the Input-oriented CCR-model.

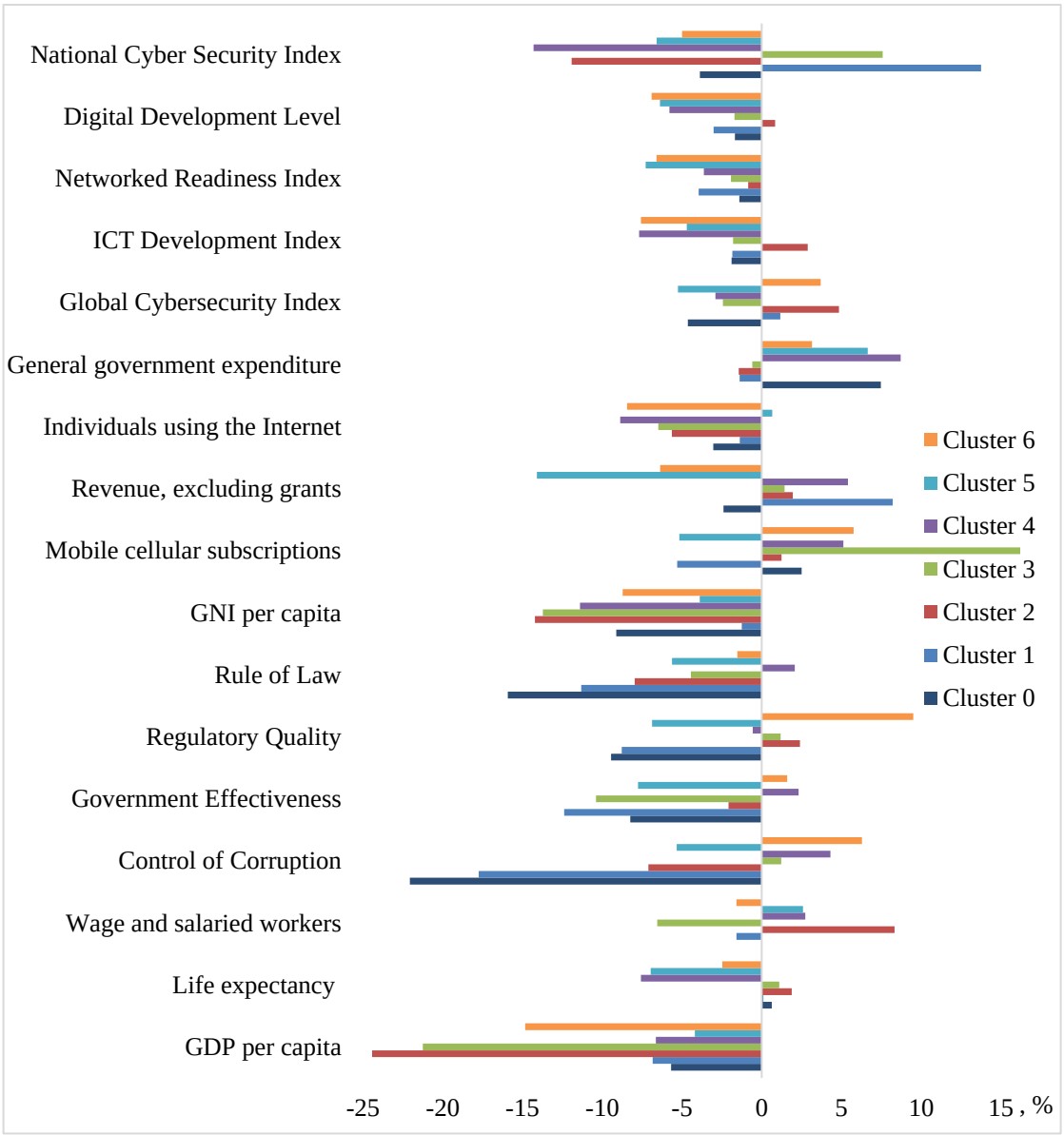

Figure 7. Comparison of the potential for improving the efficiency of the information security system of different clusters (Input-oriented CCR-model)

Source: independent development by authors.

Thus, to ensure the actual level of the index of counteraction to information threats, a number of indicators have a significant reserve, which is typical for countries in all clusters. These include GDP per capita, GNI per capita, Networked Readiness Index (see Figure 7), i.e. the level of economic potential specific to the cluster countries and the level of their technological readiness for the application of the latest information and communication technologies in the information security environment are sufficient for ensuring the current level of counteraction to information threats. As for other indicators, the improvement of the Global Cybersecurity Index (1.17%), the National Cyber Security Index (13.75%) and the Revenue, excluding grants (8.21%) is important for the countries of the first cluster). In other words, the main problem for this group is

the insufficient level of countries' commitment to cybersecurity at the global level and their readiness to counter cyber threats, as well as the insufficient level of cash receipts from taxes, social security contributions and other income.

The countries of the second cluster, which include developed and intensively developing countries, are characterized by an insufficient level of Wage and salaried workers (8.33%), Regulatory Quality: Estimate (2.4%), Mobile cellular subscriptions (1.24%), Revenue, excluding grants (1.95%), Global Cybersecurity Index (4.84%), ICT Development Index (2.89%), Digital Development Level (0.84%) (see Figure 7). To ensure the existing level of information security, the countries of this group should pay attention to those areas that relate to the development of information technology and digitalization of the country. This will help create additional jobs in the IT industry, which will lead to increased cash flow from this area.

The countries with an average economic development, which are included in the third cluster, should focus on increasing the level of Control of Corruption (1.22%), Regulatory Quality (1.19%), Mobile cellular subscriptions (16.21%), Revenue, excluding grants (1.43%), National Cyber Security Index (7.58%) (see Figure 7). The results indicate the need to introduce measures to strengthen control over corruption and improve the quality of standards in the field of information security. The most critical is the need to create conditions for personal protection of mobile users through the introduction of modern technologies. Fourth cluster countries should pay attention to improving indicators such as Wage and salaried workers (2.73%), Control of Corruption (4.31%), Government Effectiveness (2.31%), Rule of Law (2.07%) , Mobile cellular subscriptions (5.12%), Revenue, excluding grants (5.41%), General government expenditure (8.71%) (see Figure 7). This group of countries is characterized by an insufficient level of socio-economic development, which would ensure the required level of information security, which is offset by reserves of security indicators. The priorities for these countries should be measures that will help to raise the level of economy and social standards.

The countries of the 5th and 6th clusters are the least developed or have a critical level of information security system development. To ensure the current level of information security, the countries of the 5th cluster need to increase Wage and salaried workers (2.59%), Individuals using the Internet (0.66%), General government expenditure (6.65%); 6th cluster countries - Control of Corruption (6.29%), Government Effectiveness (1.6%), Regulatory Quality (9.5%), Mobile cellular subscriptions (5.76%), General government expenditure (3, 15%), Global Cybersecurity Index (3.7%) (see Figure 7). That is, there are many problems associated with the socio-economic development of these countries that need to be addressed as a matter of priority. Due to the fact that they have rather low information security indicators, which provide only the minimum basic requirements for security systems, existing IT development reserves, digitalization of the country, technological readiness and readiness to counter cyber threats is enough to maintain the actual level of information security. But the modern development of software, hardware and information tools will require other approaches, the provision of which is possible only by strengthening the socio-economic potential of the country. The results of the analysis of the effectiveness of the information security system of different clusters, considering the determination of the maximum level of the index of counteraction to information threats, obtained by building an Output-oriented CCR-model, are presented in Figure 8.

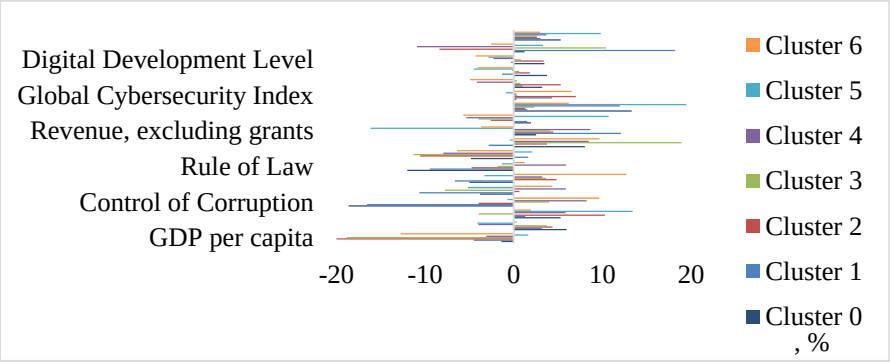

Figure 8. Comparison of the potential for improving the efficiency of the information security system of different clusters (Output-oriented CCR-model)

Source: independent development by authors.

The maximum growth of the index of information security threat for the first cluster countries is possible by 3.03%, which is likely to be provided by the existing reserves of GDP per capita (-4.52%), Control of Corruption (-16.54%), Government Effectiveness (-10.64%), Regulatory Quality (-6.65%), Rule of Law (-9.46%), Mobile cellular subscriptions (-2.81%), Networked Readiness Index (-1.32%), Digital Development Level (-0.3%) (see Figure 8). For the countries of the second cluster it is possible to increase the index of the level of information security threat by 2.62%, which is possible due to the reserves of GDP per capita (-19.99%), Control of Corruption (-3.95%), Rule of Law (-4,75%), GNI per capita (-10.55%), Individuals using the Internet (-2.59%), National Cyber Security Index (-8.38%) (see Figure 8). That is, a strong level of development of the 1st and 2nd clusters can increase the efficiency of the information security system in the country due to the conditions of effective employment of security specialists, absence of corruption, legal regulation of information security and legal responsibility for its violation, creation and use of modern software and hardware for information protection, etc.

The index of the level of information security threat for the countries of the third cluster may increase by 2.66% under the existing reserves of GDP per capita (-18.81%), Wage and salaried workers (-3.95%), Government Effectiveness (-7.78 %), Rule of Law (-1.81%), GNI per capita (-11.31%), Individuals using the Internet (-3.96%) (see Figure 8). That is, the countries of this group have a sufficient economic reserve and an effective government that will help create favorable financial conditions for the development of IT industry. For the countries of the fourth cluster the index may grow by 3.68% due to GDP per capita (-3.1%), GNI per capita (-7.95%), Individuals using the Internet (-5.35%), ICT Development Index (-4.18%), Networked Readiness Index (-0.14%), Digital Development Level (-2.29%), National Cyber Security Index (-10.9%) (see Figure 8). This group is characterized by the creation of a reserve of information technology, as this cluster includes developing countries and increasing investment in IT sector, which they consider as the most priority industry.

The fifth cluster countries may have the largest increase in the information security threat index compared to others – by 9.82%. This may be due to Control of Corruption (-0.71%), Government Effectiveness (-5.14%), Regulatory Quality (-3.31%), Rule of Law (-1.33%), Mobile cellular subscriptions (-0.4%), Revenue, excluding grants (-16.16%), Global Cybersecurity Index (-0.89%), Networked Readiness Index (-4.52%), Digital Development Level (-2, 86%) (see Fig. 8). We can say that the countries of this group have sufficient socio-economic and information-technological potential, which will not only increase the level of counteraction to information threats, but also contribute to the development of IT, digitalization of the economy and society, which will further ensure economic growth.

The existing potential of the sixth cluster countries allows the growth of the index of the level of information security threat by 2.98% due to the existing reserves of GDP per capita (-12.76%), GNI per capita (-6.37%), Revenue, excluding grants (-3,66%), Individuals using the Internet (-5.69%), ICT Development Index (-4.91%), Networked Readiness Index (-4.07%), Digital Development Level (-4.32%), National Cyber Security Index (-2.56%) (see Figure 8). That is, the countries of this group have a sufficient reserve of economic and information technology resources, which will increase the effectiveness of countering information threats.

5. Conclusion

The issue of improving the effectiveness of the information security system in terms of combating information threats is quite relevant, due to the growing level of informatization, digitalization and computerization of society. The application of Data Envelopment Analysis in this work allowed to determine the effectiveness of the information security system of the countries grouped in clusters, considering the level of their socio-economic development and the development of various areas of information security. The CCR and BBC models provided an opportunity to analyze the structural effectiveness of socio-economic development indicators and aspects of their security, taking into account the current level of the information security threat index. Also, these models allowed us to estimate the maximum level of growth of the index of information security threat with the available resource potential of the country. The CCR model proved to be more restrictive than the HRC in determining effectiveness, which helped to form a more critical assessment of the existing reserves of countries needed to counter information threats. That is why it was used to analyze all clusters of countries.

As a result, it was found that an increase in the information security threat index is possible in the range from 2.62% to 9.82%. The largest growth is characteristic of the cluster, which includes countries with low levels

of economic development. But they have significant potential for socio-economic and IT development, sufficient for strong growth and the level of counteraction to information threats. For countries that occupy leading positions in the world in terms of their high level of development, it is possible to increase the index of information security threat by 5.31%, which indicates the existence of favorable conditions for creating an effective information security system.

The analysis of structural efficiency allowed to identify those weaknesses that need change. This concerns the need to transform the information technology component for the countries of the first and second clusters, which have the prerequisites for creating comfortable conditions for attracting IT professionals, building modern enterprises for the production of computer technology, development of IT startups, etc. Countries in the zero cluster should increase public spending on security and personal protection. For countries with an average level of economic development of the third cluster, it is advisable to increase the conditions of personal protection, strengthen control over corruption, improve the quality of legislation. Insufficient level of socio-economic development of the fourth cluster countries revealed the need for economic growth and raising the level of social standards, which will stimulate the growth of information security. The least developed countries in the 5th and 6th clusters also need to pay attention to solving economic problems, which will further affect the security sphere.

It would be useful to study the effectiveness of the information security system for each individual country, which will identify specific problems for this country. In the future, it is planned to supplement the analysis of such studies, as well as to expand the number of development indicators, which will take into account those aspects that have any degree of impact on the level of information security of the country.

Acknowledgment

This work is carried out with in the tax payer – funded researches: No. 0118U003574 “Cybersecurity in the banking fraud enforcement: protection of financial service consumers and the financial and economic security growth in Ukraine”.

Funding: 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”, “Quadrocentric recrusive model of Ukrainian unshadow economy to increase its macroeconomic stability” anb “Optimization and automation of financial monitoring processes to increase information security of Ukraine”.

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. Ponemon Institute (2019). *Cost of a Data Breach Report 2019.* Retrieved from https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf.
2. IBM Security and Ponemon Institute (2020). *Cost of a Data Breach Report 2019.* Retrieved from https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf.
3. Morrow, S. and Crabtree, T. (2019). *The future of cybercrime & security. Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024.* Retrieved from Juniper Research: https://www.juniperresearch.com/researchstore/key-vertical-markets/cybercrime-cybersecurity-research-report?utm_campaign=pr1_thefutureofcybercrime_technology_aug19&utm_source=businesswire&utm_medium=pr.
4. Loshytskyi, M., Kostenko, O., Koropatnik, I., Tereshchuk, G. and Karelin V. (2020). Organizational competence of NATO information security policy. *Journal of Security and Sustainability Issues,* 9(3), 735-746. DOI: 10.9770/JSSI.2020.9.3(1).

5. Frolova, E.E., Polyakova, T.A., Dudin, M.N., Rusakova, E.P. and Kucherenko, P.A. (2018). Information security of Russia in the digital economy: The economic and legal aspects. *Journal of Advanced Research in Law and Economics*, 9(1), 89-95. DOI: 10.14505/jarle.v9.1(31).12.
6. Deane, J.K., Goldberg, D.M., Rakes, T.R. and Rees, L.P. (2019). The effect of information security certification announcements on the market value of the firm. *Information Technology and Management*, 20(3), 107-121. DOI: 10.1007/s10799-018-00297-3.
7. Kosevich, E. (2020). Cyber security strategies of Latin America countries | [Estrategias de seguridad cibernética en los países de América Latina]. *Iberoamerica (Russian Federation)*, 1, 137-159. DOI: 10.37656/S20768400-2020-1-07. [in Spanish].
8. Sorokivska, O. (2015). Economic security of ukrainian enterprises under information war. *Actual Problems of Economics*, 174(12), 198-202.
9. Jazri, H., Zakaria, O., and Chikohora, E. (2018, May). Measuring Cybersecurity Wellness Index of Critical Organisations. In *2018 IST-Africa Week Conference (IST-Africa)*. IEEE, 2018. pp. 1 - 8.
10. Yunis, M.M. and Koong, K.S. (2015). A conceptual model for the development of a national cybersecurity index: An integrated framework. In *21st Americas Conference on Information Systems, AMCIS 2015 (Puerto Rico, El Conquistador Resort and Convention CenterFajardo*), AMCIS 2015. Retrieved from https://aisel.aisnet.org/amcis2015/ISSecurity/GeneralPresentations/44/.
11. Tolubko, V., Kozelkov, S., Zybin, S., Kozlovskyi, V., & Boiko, Y. (2018, January). Criteria for evaluating the effectiveness of the decision support system. In *International Conference on Computer Science, Engineering and Education Applications* (pp. 320-330). Springer, Cham.
12. Fedotova, G.V., Kovalenko, O.A., Malyutina, T.D., Glushchenko, A.V. and Sukhinin, A.V. (2019). Transformation of information security systems of enterprises in the context of digitization of the national economy. In *Studies in Computational Intelligence* (pp. 811-822. DOI: 10.1007/978-3-030-13397-9_84).
13. Hu, Z., Khokhlachova, Y., Sydorenko, V. and Opirskyy, I. (2017). Method for optimization of information security systems behavior under conditions of influences. *International Journal of Intelligent Systems and Applications*, 9(12), 46-58. DOI: 10.5815/ijisa.2017.12.05.
14. Chen, J., Pedrycz, W., Ma, L. and Wang, C. (2014). A new information security risk analysis method based on membership degree. *Kybernetes*, 43(5), 686-698. DOI: 10.1108/K-10-2013-0235.
15. Dudykevych, V., Prokopyshyn, I., Chekurin, V., Opirskyy, I., Lakh, Y., Kret, T., Ivanchenko, Y. and Ivanchenko, I. (2019). A multicriterial analysis of the efficiency of conservative information security systems. *Eastern-European Journal of Enterprise Technologies*, 3(9-99), 6-13. DOI: 10.15587/1729-4061.2019.166349.
16. e-Governance Academy Foundation (2020). *National Cyber Security Index*. Retrieved from NCSI: https://ncsi.ega.ee/ncsi-index/.
17. The World Bank (2020). *World Development Indicators.* Retrieved from https://databank.worldbank.org/source/world-development-indicators/Type/TABLE/preview/on.
18. Yarovenko, H. (2020a). Use of Kohonen maps to analyze the information security level of countries taking into account their development | [Vykorystannia kart Kokhonena dlia analizu rivnia informatsiinoi bezpeky krain z urakhuvanniam yikh rozvytku]. *Economic space*, 157, 118-124. DOI: 10.32782/2224-6282/157-21. [in Ukrainian]
19. Yarovenko, H. (2020b). Evaluating the threat to national information security. *Problems and Perspectives in Management*, 18(3), 195-210. DOI: 10.21511/ppm.18(3).2020.17.
20. Charnes, A., Cooper, W.W. and Rhodes, E. (1978). Measuring the efficiency of decision making units. *European Journal of Operational Research*, 2, 429-444.
21. Banker, R.D., Charnes, A. and Cooper, W.W. (1984). Some Models for Estimating Technical and Scale Inefficiencies in Data Envelopment Analysis. *Managment Science*, 30(9), 1031-1142. DOI: 10.1287/mnsc.30.9.1078.
22. Banxia Software (2020). *Frontier Analyst.* Retrieved from https://banxia.com/frontier/resources/demodownload/.