“Evaluating the threat to national information security”

AUTHORS	Hanna Yarovenko https://orcid.org/0000-0002-8760-6835 http://www.researcherid.com/rid/P-3734-2014

ARTICLE INFO	Hanna Yarovenko (2020). Evaluating the threat to national information security. *Problems and Perspectives in Management*, *18*(3), 195-210. doi:10.21511/ppm.18(3).2020.17
DOI	http://dx.doi.org/10.21511/ppm.18(3).2020.17
RELEASED ON	Wednesday, 09 September 2020
RECEIVED ON	Wednesday, 10 June 2020
ACCEPTED ON	Friday, 28 August 2020

JOURNAL	"Problems and Perspectives in Management"
ISSN PRINT	1727-7051
ISSN ONLINE	1810-5467
PUBLISHER	LLC “Consulting Publishing Company “Business Perspectives”
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
34	5	6

BUSINESS PERSPECTIVES

LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10,
Sumy, 40022, Ukraine

www.businessperspectives.org

Hanna Yarovenko (Ukraine)

EVALUATING THE THREAT TO NATIONAL INFORMATION SECURITY

Abstract

An effective strategy for managing the national information security with capabilities to resist information threats significantly impacts its further development. This study aims to assess the level of threat to the information security of countries based on the integral index. It is proposed to use five indicators characterizing individual areas of information security and 37 world development indicators, selected from the World Bank database. Correlation analysis selected 12 out of 37 development indicators relevant to security indicators for which the correlation coefficient exceeded 0.5 or –0.5. The Harrington-Mencher function is proposed to determine the information security threat index. Nonlinear normalization was carried out to bring the initial data to a comparable measurement. Canonical analysis was performed to determine the indicator weights. The data from 159 countries were taken for 2018 to assess the index. The result was presented on the map showing countries' distribution by the information security threat index, thus forming five groups. The group with a "very well" resistance to threats includes economically developed countries with a high level of information security. The "well" group was formed by new industrial and developing countries with economic potential sufficient to prevent information threats and combat their consequences. The information security level in developing countries, where the results of overcoming information threats will affect the economic sphere, is defined as "acceptable". Countries with a low level of development and information security formed groups designated as "bad" and "very bad", which indicates a high level of threats to their information security.

Keywords canonical analysis, correlation, Harrington-Mencher function, index, information, threat, security

JEL Classification C10, C43, O30

Received on: 10th of June, 2020
Accepted on: 28th of August, 2020
Published on: 9th of September, 2020

Hanna Yarovenko, Ph.D. in Economics, Associate Professor, Economic Cybernetics Department, Sumy State University, Ukraine.

Conflict of interest statement:
Author(s) reported no conflict of interest

INTRODUCTION

No sphere of human activity is carried out without digital and computer technologies, caused by the critical growth of information that requires processing, analysis, and effective use. On the other hand, increased information flows generate the risk of using information for criminal purposes. At the national level, this can lead to information wars, cyber-terrorist operations to steal classified information, the disclosure of personal data of clients of companies, banks, etc. As a result, such actions can violate the balance of social attitudes in society, the balance of political forces, can lead to financial losses for large companies, change the attitude of international funds, organizations, and investors towards cooperation with such countries. As a result, there is a decrease in government administration efficiency, which leads to the inhibition of its development.

The issues related to information security are relevant not only for government agencies but also for business entities and the country's population. Accordingly, the consequences of information wars, cyber terrorism, massive hacker attacks, and other threats can affect the country as a whole and an individual or a company. The results of

this impact can also be manifested in various fields of activity. Thus, many fraudsters are trying to take advantage of the situation developed in the world due to the COVID 19 pandemic and send fake links with information about the virus on behalf of the World Health Organization. Many people lost their personal and payment information, and fraudsters gained access to their accounts (Anscombe, 2020). At the end of July 2020, 280,000 of 1,45 million profiles in the DNA database of the website "GEDmatch" were hacked, making them accessible to hackers and third parties (Aldhous, 2020). In 2019, employees of 27% of companies worldwide became targets of cyber terrorists due to the use of smartphone software (Dumas, 2020). Such cases lead to an increase in companies' financial losses, a decrease in the level of public confidence in those institutions that have access to personal information. Thus, the losses of companies around the world as a result of a breach of their information security and overcoming the consequences in 2018 amounted to about USD 3 trillion, and their growth is predicted to USD 5 trillion in 2024 (Morrow & Crabtree, 2019), which indicates an increase in the level of information threats in the future.

Considering the problems of information security, one of the priorities for the country's further development is an effective information security management strategy that will provide a mechanism for determining its level and predicting the ability to reveal and counteract information threats. Therefore, this issue requires a comprehensive study in terms of national security and development.

1. LITERATURE REVIEW

Scientists from all over the world are researching information security issues. To analyze their scientific works, a bibliometric map was constructed based on papers from the Scopus database (Scopus, 2020) using the VOSviewer software product (VOSviewer, 2020). The map was constructed based on the clusters of keywords used in scientific publications and related to information security and economics (Figure 1).

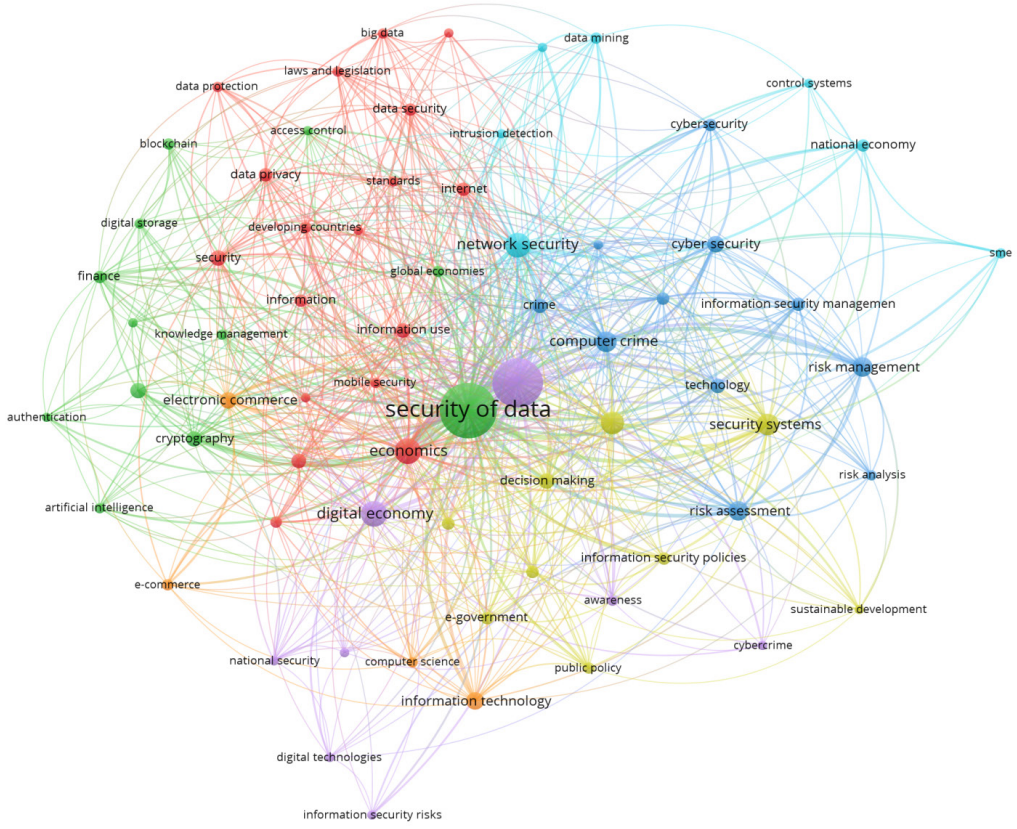

Figure 1. Bibliometric map constructed based on keywords from publications on the Scopus database

http://dx.doi.org/10.21511/ppm.18(3).2020.17

The map shows 7 clusters of publications (Figure 1), each highlighted in a different color. The red cluster is formed by studies highlighting a wide range of general issues related to information security. They include those devoted to the development of economics, law, standardization, and the development of strategies in this area. Thus, Topa and Karyda (2019) provide guidance on developing standards to improve its information security management practices. Kosevich (2020) offers examples of information security strategies that consider the specifics of the country's development. Dincelli (2018) highlights the impact of cultural differences on information security and the development of an appropriate strategy to combat information threats. Negative consequences in the information environment and violation of the national political stability can cause external political conflicts (Kirilenko & Alexeyev, 2018). As part of the emergence of internal conflicts, the persecution of freedom of speech can pose a threat to the country's information security, which requires a review of legal aspects (Omirzhanov et al., 2017). Park (2019) also notes that legislation's ineffectiveness is one of the reasons for the violation of information security within the state by business entities.

The green cluster (Figure 1) reflects research related to blockchain technology, artificial intelligence, cryptography, cloud technology, knowledge management, etc. This cluster explores the possibilities of various modern technologies for information protection in economics, finance, and management. Klyaus and Gatchin (2020) suggest using the mathematical model for information security controls optimization and evaluating the information security systems' effectiveness using the gradient method. Fuzzy logic method can be used to protect personal data (Dorosh, Voitsekhovska, & Balchenko, 2019). For more complex systems, Schmitz and Pape (2020) recommend using comprehensive approaches, one of which is a lightweight, domain-specific framework to support information security decision-making. One of the promising methods may be blockchain technology (Warkentin & Orgeron, 2020). Brožová, Šup, Rydval, Sadok, and Bednar (2016) apply the semantic network to develop a decision-making network and network process that considers qualitative and quantitative data.

The blue cluster (Figure 1) concerns information security management, cybercrime, risk, and personal security research. It also covers works that highlight security issues for society and risk management issues related to cyber threat warnings. Within the framework of this cluster, the success factors of information security management of small and medium-sized enterprises are investigated, namely the compliance of information security management with the company's business activities, support of top management, security controls, and organizational awareness, with the emphasis on organizational awareness (Ključnikov, Mura, & Sklenár, 2019). Singh and Gupta (2019) also emphasize the importance of top management support, organizational information security culture, and proper monitoring system for information security management. As one of the effective information security management measures, Bekmuratov et al. (2020) proposed the concept of building an automated information security system at the enterprise.

The yellow cluster (Figure 1) reflects the research on information security management, policy, and investment. Publications of this cluster reveal the problems of information management and the development of appropriate measures. Thus, Frolova, Polyakova, Dudin, Rusakova, and Kucherenko (2018) highlight possible measures that ensure the management of the information security system at the micro and macro levels in the applied and legal aspect. The results of ineffective information security management at the national level can lead to a decrease in any state's investment attractiveness. As a result, this will negatively affect the development of the national economy, which is the subject of research by Cardholm (2015). Therefore, it is important to develop information security management programs, investment in which increases companies' value and creates a favorable investment climate in the country (Deane, Goldberg, Rakes, & Rees, 2019). Burke, Oseni, Jolfaei, and Gondal (2019) suggest using cybersecurity indices to measure it in the health care sector, Yunis and Koong (2015) – a comprehensive cybersecurity index that takes into account many factors. Jazri, Zakaria, and Chikohora (2018) focus on creating a cybersecurity improvement index. Popova, Korostelkina, Dedkova, and Korostelkin (2019) study the indicators of its development in the

conditions of digitalization of the economy. In practice, to improve the efficiency of information security management in countries, several indicators are used that characterize certain areas of information security. They include the Global Cybersecurity Index, the National Cyber Security Index (e-Governance Academy Foundation, 2020), which allows assessing the priority areas needed to improve the national cybersecurity. These indicators are calculated according to different metrics and methods and show the country's rating among other states of the world. In contrast, the country may have radically different positions according to these indices, leading to difficulties in developing an information security strategy at the national level. It should be noted that the process of determining indicators related to information security does not take into account the aspect of the economic, social, and political development of the state. This is important for those cases when information security threats arise in the country, and knowledge of the development level will help develop a forecast of how the country will be able to quickly respond and recover after the information crisis.

The fifth cluster of publications (lilac) highlights the aspect of national security for the digital economy, i.e., reveals the issues of information protection and control in this area. Thus, Sonny (2011) examines the concept of national security in the context of its growing dependence on information technologies. Kshetri (2017) examines the imperatives of the US National Cyber Commission's Report on the Provision and Growth of the Digital Economy, which was developed in response to the rise in cyber threats.

The sixth and seventh clusters are small and reflect aspects of cyber threat detection systems, network security, data mining, and relate to e-commerce, i.e., they outline specific areas.

The analysis of research conducted by foreign scientists shows various approaches to the problem of information security. One can highlight the yellow cluster publications concerning the use of indexes in the framework of information security management strategies. However, the problem is that these indicators are used to evaluate certain areas of information security, such as cybersecurity. Information security is a complex concept that covers security at the macro and micro levels, and also includes the legislative framework, agencies that ensure information security, software and hardware, security policy, and industry professionals. At the same time, its level is affected by the development of the country. Therefore, to assess the level of its threat, it is necessary to consider the complexity of this concept.

2. AIMS

This study aims to assess the level of threat to national information security based on the integral index, which considers the indicators of its development and information security.

3. METHODOLOGY AND DATA

3.1. Data collection

The integral index of the threat to the national information security is an indicator that summarizes, on the one hand, the characteristics inherent in the national information security system regarding its capabilities to prevent cyber threats, and, on the other hand, the characteristics that represent the development of the country. Therefore, it is important to consider both characteristics when calculating the index. That is why two groups of indicators were chosen. The first group was formed by indices used to assess individual areas of the national information security: Global Cybersecurity Index measures the level of cybersecurity for the member countries of the International Telecommunication Union; the National Cyber Security Index determines the level of readiness to counter cyber threats; ICT Development Index characterizes the level of development of information technologies in the country; the Networked Readiness Index measures the degree of a country's technological readiness to apply the latest information and communication technologies in various fields; Digital Development Level characterizes the level of digitalization of the country (e-Governance Academy Foundation, 2020). Each of these indicators is in-

http://dx.doi.org/10.21511/ppm.18(3).2020.17

tegral and allows evaluating the state information security management system in terms of its software, technical, and information support.

Indicators from the World Bank database were studied to form the indicators of the second group (The World Bank, 2020). Applying the methods of scientific knowledge (analysis, synthesis and deduction) to the subject area, 37 indicators were selected that characterize the development of the country (see Appendix) and can affect information security. This enabled us to assume that there is a connection between the selected development indices and security indicators. To prove its presence or absence, a correlation analysis was carried out in the STATISTICA analytical package (StatSoft, 2020) for data from 159 countries up to 2018. The number of countries and the period is determined by the availability and completeness of data for each of the selected indicators in the World Bank and e-Governance Academy Foundation databases. The results of the correlation analysis are shown in Figure 2.

Figure 2 shows the values of correlation coefficients for 37 selected indicators of the country's development in the context of five indices of information security. For further research, only relevant indicators should be selected for which the value of the correlation coefficient is approximately equal to or greater than 0.5 or –0.5, which will indicate a close relationship between the indicators. Thus, indicators 1, 2, 5, 8, 10, 11, 13, 14, 20, 26, 27, and 30 were selected according to this criterion and will be used to develop the integral index.

3.2. Research methodology

The calculation of the information security threat index includes the following stages.

Stage 1. Normalization of the input data array for comparing different measured indicators. There are many normalization methods, but nonlinear normalization was chosen for the first stage, which more efficiently smoothes the data with dif-

Note: Numbers 1-37 correspond to the ID of development indicators listed in Appendix.

Figure 2. Results of correlation analysis

ferent signs and values. This process will occur according to the formula (1):

$$Z_{ij} = \left(1 + e^{\frac{\overline{y_J} - y_{ij}}{\sigma(y)}}\right)^{-1}, \quad (1)$$

where Z_{ij} – the normalized value of the *j*-th component of the information security threat index in the context of the *i*-th country; y_J – the average value of the *j*-th component of the information security threat index within the studied list of countries; y_{ij} – the actual value of the *j*-th component of the information security threat index in the context of the *i*-th country; $\sigma\left(y_j\right)$ – the standard deviation of the *j*-th component of the information security threat index within the studied list of countries.

Stage 2. Investigation of the impact of security indicators on each of the selected indicators of the national development to determine a part of the variation of the information security threat index. To determine the impact, it is proposed at this stage to carry out a canonical analysis used to determine the dependencies between sets of variables to assess the degree of impact of one set on another. The general idea of the analysis is represented by the formula (2):

$$\begin{aligned} a_1u_1 &= b_{1_1}x_1 + b_{1_2}x_2 + b_{1_3}x_3 + b_{1_4}x_4 + b_{1_5}x_5 \\ a_2u_2 &= b_{2_1}x_1 + b_{2_2}x_2 + b_{2_3}x_3 + b_{2_4}x_4 + b_{2_5}x_5 \\ a_3u_3 &= b_{3_1}x_1 + b_{3_2}x_2 + b_{3_3}x_3 + b_{3_4}x_4 + b_{3_5}x_5 \\ &\cdots \\ a_{12}u_{12} &= b_{12_1}x_1 + b_{12_2}x_2 + b_{12_3}x_3 + b_{12_4}x_4 + b_{12_5}x_5 \end{aligned}, \quad (2)$$

where $u_1, u_2, \ldots, u_{12}$ – a set of the values of variables that reflect the selected indicators of the country's development; x_1, x_2, x_3, x_4, x_5 – weighted sums of variables, which are canonical variables and reflect five indicators characterizing the level of the country's information security; a_1, a_2, …, a_{12}, b_{1_1}, b_{1_2}, …, b_{1_5}, …, b_{12_1}, b_{12_2}, …, b_{12_5} – weighting factors that are calculated based on the maximum correlation of both sets.

Stage 3. Construction of an integral multiplicative index of information security threat based on the use of the Harrington-Mencher function, which allows measuring the effectiveness of any system in contrast to other methods (Harrington, 1965; Mencher & Zemshman, 1986).

Step 3.1. Transformation of the normalized values of the indicators of the study's statistical base into the dimensionless Harrington desirability scale using the formula (3):

$$d_{ij} = \exp\left(-\exp\left(-Z_{ij}\right)\right), \quad (3)$$

where Z_{ij} – the normalized value of the *j*-th indicator of the information security threat index in the context of the *i*-th country; d_{ij} – the intermediate value of the *j*-th indicator of the information security threat index in the context of the *i*-th country, reduced to the dimensionless Harrington desirability scale.

Step 3.2. Visualization of the dependence d_{ij} on actual values in each input indicator's context to further select the type of Harrington-Mencher transformation curve.

Step 3.3. Formalization of the Harrington-Mencher transformation within the limits of the dependence d_{ij} chosen at the previous step on the actual values in each input indicator's context. Thus, based on the graphs obtained at step 3.2, 6 types of curves can be obtained (formulae 4-9).

The first type of the curve: *S*-shaped growth, symmetric curve:

$$d_{ij}^{*} = \exp\left(-\exp\left(-9\left(\frac{Z_{ij} - \min\limits_i Z_{ij}}{\max\limits_i Z_{ij} - \min\limits_i Z_{ij}}\right)^{1.927} - 2\right)\right), \quad (4)$$

where d_{ij}^{*} – intermediate value of the *j*-th indicator of the information security threat index in the context of the *i*-th country, reduced to the dimensionless Harrington-Mencher desirability scale; $\min\limits_i Z_{ij}$ – the minimum value of the normalized *j*-th indicator of the information security threat index in the context of the *i*-th country; $\max\limits_i Z_{ij}$ – the maximum value of the normalized *j*-th indicator of the information security threat index in the context of the *i*-th country.

The second type of the curve: S-shaped growth, asymmetric curve with rapid initial growth:

http://dx.doi.org/10.21511/ppm.18(3).2020.17

$$d_{ij}^{*} = \exp\left(-\exp\left(-9\left(\frac{Z_{ij} - \min\limits_{i} Z_{ij}}{\max\limits_{i} Z_{ij} - \min\limits_{i} Z_{ij}}\right)^{k_{II}} - 2\right)\right),$$

$$k_{II} = \frac{\ln\left(2 - \ln\ln\frac{1}{d_{ij}^{II}}\right)}{\ln\left(y_{ij}^{II} - \min\limits_{i} Z_{ij}\right) - \ln\left(\max\limits_{i} Z_{ij} - \min\limits_{i} Z_{ij}\right)}, \quad (5)$$

where d_{ij}^{II}, y_{ij}^{II} – any comparable pair within the same country within the same indicator.

The third type of the curve: S-shaped growth, asymmetric curve with slow initial growth:

$$d_{ij}^{*} = 1 - \exp\left(-\exp\left(-9\left(\frac{\max\limits_{i} Z_{ij} - Z_{ij}}{\max\limits_{i} Z_{ij} - \min\limits_{i} Z_{ij}}\right)^{k_{III}} - 2\right)\right),$$

$$k_{III} = \frac{\ln\left(2 - \ln\ln\frac{1}{1 - d_{ij}^{III}}\right) - \ln 9}{\ln\left(\max\limits_{i} Z_{ij} - y_{ij}^{III}\right) - \ln\left(\max\limits_{i} Z_{ij} - \min\limits_{i} Z_{ij}\right)}, \quad (6)$$

where d_{ij}^{III}, y_{ij}^{III} – any comparable pair within the same country within the same indicator.

The fourth type of the curve: S-shaped, falling, symmetric curve:

$$d_{ij}^{*} = \exp\left(-\exp\left(-9\left(\frac{\max\limits_{i} Z_{ij} - Z_{ij}}{\max\limits_{i} Z_{ij} - \min\limits_{i} Z_{ij}}\right)^{1.927} - 2\right)\right). \quad (7)$$

The fifth type of the curve: S-shaped, falling, asymmetric curve with rapid initial decline:

$$d_{ij}^{*} = 1 - \exp\left(-\exp\left(-9\left(\frac{\max\limits_{i} Z_{ij} - Z_{ij}}{\max\limits_{i} Z_{ij} - \min\limits_{i} Z_{ij}}\right)^{k_{V}} - 2\right)\right),$$

$$k_{V} = \frac{\ln\left(2 - \ln\ln\frac{1}{1 - d_{ij}^{V}}\right) - \ln 9}{\ln\left(y_{ij}^{V} - \min\limits_{i} Z_{ij}\right) - \ln\left(\max\limits_{i} Z_{ij} - \min\limits_{i} Z_{ij}\right)}, \quad (8)$$

where d_{ij}^{V}, y_{ij}^{V} – any comparable pair within the same country within the same indicator.

The sixth type of the curve: S-shaped, falling, asymmetric curve with slow initial decline:

$$d_{ij}^{*} = \exp\left(-\exp\left(-9\left(\frac{\max\limits_{i} Z_{ij} - Z_{ij}}{\max\limits_{i} Z_{ij} - \min\limits_{i} Z_{ij}}\right)^{k_{VI}} - 2\right)\right),$$

$$k_{VI} = \frac{\ln\left(2 - \ln\ln\frac{1}{1 - d_{ij}^{VI}}\right) - \ln 9}{\ln\left(y_{ij}^{VI} - \min\limits_{i} Z_{ij}\right) - \ln\left(\max\limits_{i} Z_{ij} - \min\limits_{i} Z_{ij}\right)}, \quad (9)$$

where d_{ij}^{VI}, y_{ij}^{VI} – any comparable pair within the same country within the same indicator.

Step 3.4. Calculating the integral multiplicative index of information security threat based on the use of the Harrington-Mencher function as the geometric mean of the derivatives of the values of information security indicators and weighted indicators of the country's development:

$$IZIBNE_{i} = 1 - \sqrt[n+m]{\prod_{j=1}^{n}\left(d_{ij}^{*}\right)^{\frac{w_j}{100}} \cdot \prod_{j=n+1}^{m} d_{ij}^{*}}, \quad (10)$$

where $IZIBNE_{i}$ – integrated information security threat index for the i-th country; n – the number of indicators of country's development; m – number of information security indicators; w_{j} – the degree of variation in the information security threat index under the influence of the j-th input indicator of country's development; d_{ij}^{*} – the intermediate value of the j-th indicator of the information security threat index in the context of the i-th country, reduced to the dimensionless Harrington-Mencher desirability scale.

Stage 4. Visualization of calculation results and high-quality interpretation of the information security threat index. For this purpose, the following interpretation estimates presented in Table 1 are used.

Table 1. Quantitative and qualitative interpretation of the information security threat level index

Qualitative interpretation	Quantitative assessment
Very bad	1.00–0.80
Bad	0.80–0.63
Acceptable	0.63–0.37
Well	0.37–0.20
Very well	0.20–0.00

4. RESULTS AND DISCUSSION

The proposed approach for determining the integral indicator of the threat to national information security was consistently implemented for the selected empirical data. Thus, at the first stage, applying formula (1), normalized data were obtained for indicators of development and security indicators after normalization using MS Excel. A fragment of the results is shown in Table 2.

In the second stage, the STATISTICA analytical package was used for a canonical analysis of the interdependence of security indicators and indicators of the country's development. The results are systematized in Table 3.

"Canonical *R*" column in Table 3 shows a strong relationship between security indicators and development factors, and for most factors ($R \geq 0.7$), while the relationship is significant for "Life expectancy", "Mobile cellular subscriptions", and "Revenue, excluding grants" since $0.7 > R \geq 0.5$. Its statistical significance is confirmed by the high value of the Pearson test ("Chi-square" column), the significance level of which does not exceed

Table 2. Normalized components of the information security threat index (fragment)

Country	GDP per capita	Life expectancy	Wage and salaried workers	...	Networked Readiness Index	Digital Development Level	National Cyber Security Index
Afghanistan	0.3282	0.3525	0.1906	...	0.1402	0.1637	0.2576
Albania	0.3807	0.6319	0.3718	...	0.5755	0.5082	0.5315
Algeria	0.3676	0.5975	0.5851	...	0.4816	0.4192	0.2778
Angola	0.3600	0.2865	0.2642	...	0.1402	0.1631	0.2383
Antigua and Barbuda	0.5169	0.6013	0.1123	...	0.1402	0.5513	0.2576
Argentina	0.4560	0.5941	0.6366	...	0.5570	0.5989	0.5947
Armenia	0.3687	0.5626	0.5114	...	0.6210	0.5802	0.4290
Australia	0.8844	0.7095	0.7069	...	0.7640	0.7939	0.7000
Austria	0.8519	0.6904	0.7384	...	0.7500	0.7789	0.7699
Azerbaijan	0.3745	0.5201	0.2798	...	0.6210	0.6061	0.4928
...	...	...	...	...	...	...	...
United Kingdom	0.7919	0.6854	0.7167	...	0.7773	0.8202	0.8275
United States	0.9089	0.6334	0.7755	...	0.7901	0.8082	0.8348
Uruguay	0.5235	0.6186	0.6146	...	0.6473	0.6760	0.5947
Uzbekistan	0.3391	0.4936	0.4799	...	0.1402	0.4527	0.4290
Vanuatu	0.3565	0.4680	0.2537	...	0.1402	0.2296	0.2478
Venezuela	0.3227	0.5050	0.5283	...	0.5099	0.4665	0.4417
Vietnam	0.3504	0.5701	0.3689	...	0.5755	0.4650	0.4544
Yemen	0.3327	0.3833	0.4014	...	0.1402	0.0702	0.2291
Zambia	0.3392	0.3344	0.2127	...	0.4816	0.3002	0.5315
Zimbabwe	0.3458	0.2935	0.3026	...	0.4533	0.3051	0.2882

Table 3. Results of canonical analysis

Indicators	Total redundancy	Canonical R	Chi-square	p
GDP per capita	52.21	0.7226	114.09	6.172276000000000E-23
General government expenditure	36.39	0.6033	69.91	0.000000000000111074
Life expectancy	32.91	0.5737	61.67	0.000000000005628692
Wage and salaried workers	58.41	0.7643	135.54	1.820447000000000E-27
Control of corruption: estimate	56.38	0.7509	128.21	6.450657000000000E-26
Government effectiveness: estimate	75.61	0.8696	218.02	0.00
Regulatory quality: estimate	72.17	0.8495	197.63	0.00
Rule of law: estimate	59.90	0.7739	141.17	1.170979000000000E-28
GNI per capita	62.90	0.7931	153.20	0.00
Mobile cellular subscriptions	42.29	0.6503	84.94	8.174966000000000E-17
Revenue, excluding grants	39.36	0.6274	77.29	3.224691000000000E-15
Individuals using the Internet	86.01	0.9274	303.85	0.00

http://dx.doi.org/10.21511/ppm.18(3).2020.17

0.05 (p = 0.0000). The column "Total redundancy" presents the values of redundancy for indirect impact factors, which are explained by the variability of information security indicators. For example, the indicator "GDP per capita" by 52.21% is explained by changes in information security indicators, i.e., their variation leads to a change in GDP per capita by 52.21%. Since development factors influence the country's level of information security indirectly, the obtained values of variability will allow using them as weights of the impact of these indicators when calculating the integral indicator of information security.

At step 3.1, the statistical database indicators' normalized values were transformed into the dimensionless Harrington desirability scale using the formula (3). A fragment of the obtained data is shown in Table 4.

At step 3.2, for each component of the information security threat index, a graph is constructed, and the shape's analysis made it possible to determine the type of curve. As a result, 17 graphs were obtained, the dependencies on which were identified only by two types of curves. Thus, the second type of the curve is characteristic of the following indicators: GDP per capita; GNI per capita; Revenue, excluding grants; Networked Readiness Index; National Cyber Security Index. An example of the result obtained for the GDP per capital indicator is shown in Figure 3. For all other indicators, the first type of the curve was identified, an example of which for the Control of corruption: estimate indicator is shown in Figure 4. The choice of the type of curve allowed for a further transformation of the Harrington-Mencher function, which is used to determine the integrated index of information security threats.

Based on the preliminary step results, for indicators with the first type of the curve, formula 4 was chosen for calculation d_{ij}^{*}, and for indicators with a curve of the second type, formula 5 was chosen. The corresponding calculations were carried out in MS Excel, a fragment of which is shown in Table 5.

In the process of calculating the Harrington-Mencher transformations for a curve of the second type, it was necessary to determine d_{ij}^{II}, y_{ij}^{II}, (formula 5). For this purpose, the data were taken for a comparable country. The countries with the

Table 4. The values of components of the information security threat index reduced to the dimensionless Harrington desirability scale (fragment)

Country	GDP per capita	Life expectancy	Wage and salaried workers	...	Networked Readiness Index	Digital Development Level	National Cyber Security Index
Afghanistan	0.4866	0.4951	0.4376	...	0.4193	0.4279	0.4617
Albania	0.5049	0.5877	0.5018	...	0.5698	0.5480	0.5556
Algeria	0.5004	0.5769	0.5729	...	0.5391	0.5181	0.4689
Angola	0.4977	0.4719	0.4640	...	0.4193	0.4276	0.4548
Antigua and Barbuda	0.5508	0.5781	0.4091	...	0.4193	0.5620	0.4617
Argentina	0.5306	0.5758	0.5891	...	0.5639	0.5773	0.5760
Armenia	0.5008	0.5657	0.5490	...	0.5843	0.5713	0.5214
Australia	0.6617	0.6115	0.6107	...	0.6276	0.6363	0.6086
Austria	0.6527	0.6057	0.6201	...	0.6235	0.6320	0.6294
Azerbaijan	0.5028	0.5519	0.4696	...	0.5843	0.5796	0.5429
...	...	...	...	...	...	...	...
United Kingdom	0.6357	0.6042	0.6136	...	0.6315	0.6438	0.6459
United States	0.6683	0.5882	0.6310	...	0.6352	0.6404	0.6479
Uruguay	0.5530	0.5835	0.5823	...	0.5925	0.6013	0.5760
Uzbekistan	0.4905	0.5431	0.5386	...	0.4193	0.5295	0.5214
Vanuatu	0.4965	0.5346	0.4603	...	0.4193	0.4516	0.4582
Venezuela	0.4847	0.5469	0.5545	...	0.5485	0.5341	0.5257
Vietnam	0.4944	0.5681	0.5008	...	0.5698	0.5336	0.5300
Yemen	0.4882	0.5058	0.5120	...	0.4193	0.3937	0.4515
Zambia	0.4905	0.4888	0.4456	...	0.5391	0.4768	0.5556
Zimbabwe	0.4928	0.4744	0.4777	...	0.5297	0.4785	0.4725

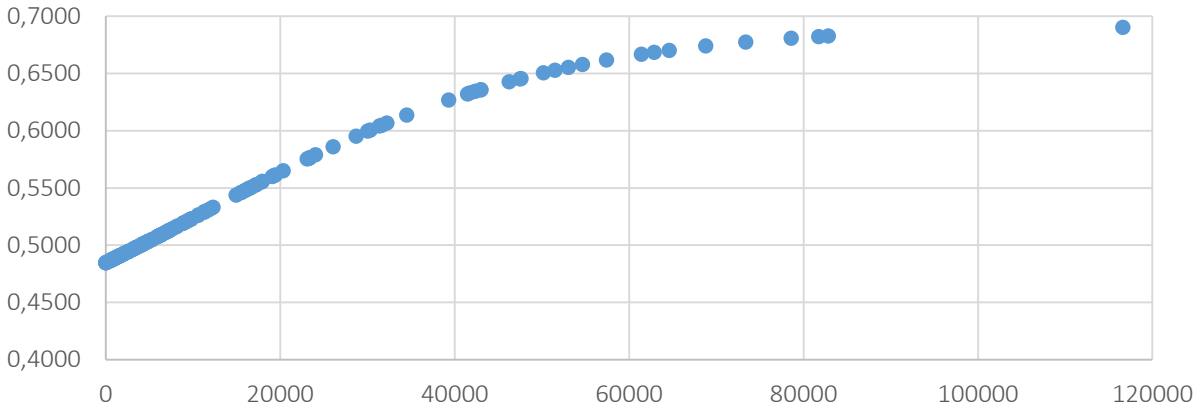

Figure 3. Graph of the second type of the curve for GDP per capita

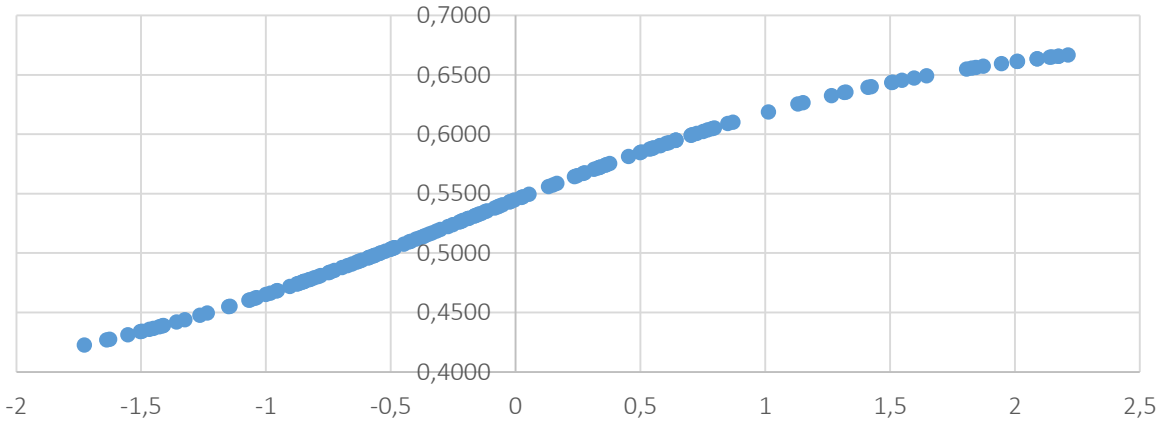

Figure 4. Graph of the first type of curve for Control of corruption: estimate

average value of the corresponding indicator were selected, as this reduced the gap between the countries with the highest and lowest indicators of development and security. Based on the transformations, the integral index of information security threat was calculated using formula 10, and a map of the distribution of countries by the index of information security threat was constructed (Figure 5).

As a result, five groups of countries were obtained; the level of the country's development and information security are determined by their ability to counter threats to information security. Thus, 47 countries have a "very well" level of counteraction to threats: Western, Northern, and Southern Europe, the United States, Canada, Australia, Japan, New Zealand, Malaysia, Saudi Arabia, Israel, etc. (Figure 5). This group was formed by countries that are mostly developed, have a strong economy, high scientific and technical potential, apply strategic approaches to information security management at the country level. They have the highest opportunities compared to other countries to counter cyber threats, information terrorism, which decreases the status of protecting national interests and personal interests. Therefore, they have great advantages over others in terms of response speed in the case of destabilization of the level of information security and have the resources to recover, which will not affect further development.

According to the results, 20 countries were assigned to the group with a qualitative rating of "well". It was formed by several new industrial countries – Brazil, China, the Philippines, South Africa, Thailand, Turkey, and several developing countries – Albania, Argentina, Armenia, Kazakhstan, the Russian Federation, etc. These countries have

http://dx.doi.org/10.21511/ppm.18(3).2020.17

Table 5. Calculations of Harrington-Mencher transformation values (fragment)

Country	GDP per capita	Life expectancy	Wage and salaried workers	...	Networked Readiness Index	Digital Development Level	National Cyber Security Index
Afghanistan	0.0040	0.4320	0.0016	...	0.0006	0.0018	0.9632
Albania	0.2115	0.9913	0.1447	...	0.9980	0.7230	0.9963
Algeria	0.1332	0.9827	0.9008	...	0.9969	0.3743	0.9730
Angola	0.0934	0.1778	0.0102	...	0.0006	0.0018	0.9472
Antigua and Barbuda	0.8340	0.9840	0.0006	...	0.0006	0.8397	0.9632
Argentina	0.6470	0.9816	0.9599	...	0.9978	0.9205	0.9973
Armenia	0.1393	0.9667	0.7102	...	0.9983	0.8942	0.9933
Australia	0.9974	0.9984	0.9902	...	0.9990	0.9980	0.9982
Austria	0.9963	0.9975	0.9951	...	0.9989	0.9973	0.9986
Azerbaijan	0.1730	0.9301	0.0158	...	0.9983	0.9292	0.9955
...	...	...	...	...	...	...	...
United Kingdom	0.9931	0.9972	0.9921	...	0.9990	0.9989	0.9988
United States	0.9979	0.9916	0.9979	...	0.9990	0.9986	0.9989
Uruguay	0.8472	0.9886	0.9402	...	0.9985	0.9787	0.9973
Uzbekistan	0.0196	0.8930	0.5847	...	0.0006	0.5140	0.9933
Vanuatu	0.0774	0.8432	0.0076	...	0.0006	0.0088	0.9563
Venezuela	0.0006	0.9106	0.7671	...	0.9973	0.5705	0.9939
Vietnam	0.0524	0.9709	0.1366	...	0.9980	0.5641	0.9943
Yemen	0.0088	0.5644	0.2419	...	0.0006	0.0006	0.9348
Zambia	0.0198	0.3545	0.0026	...	0.9969	0.0501	0.9963
Zimbabwe	0.0369	0.1998	0.0292	...	0.9965	0.0558	0.9765

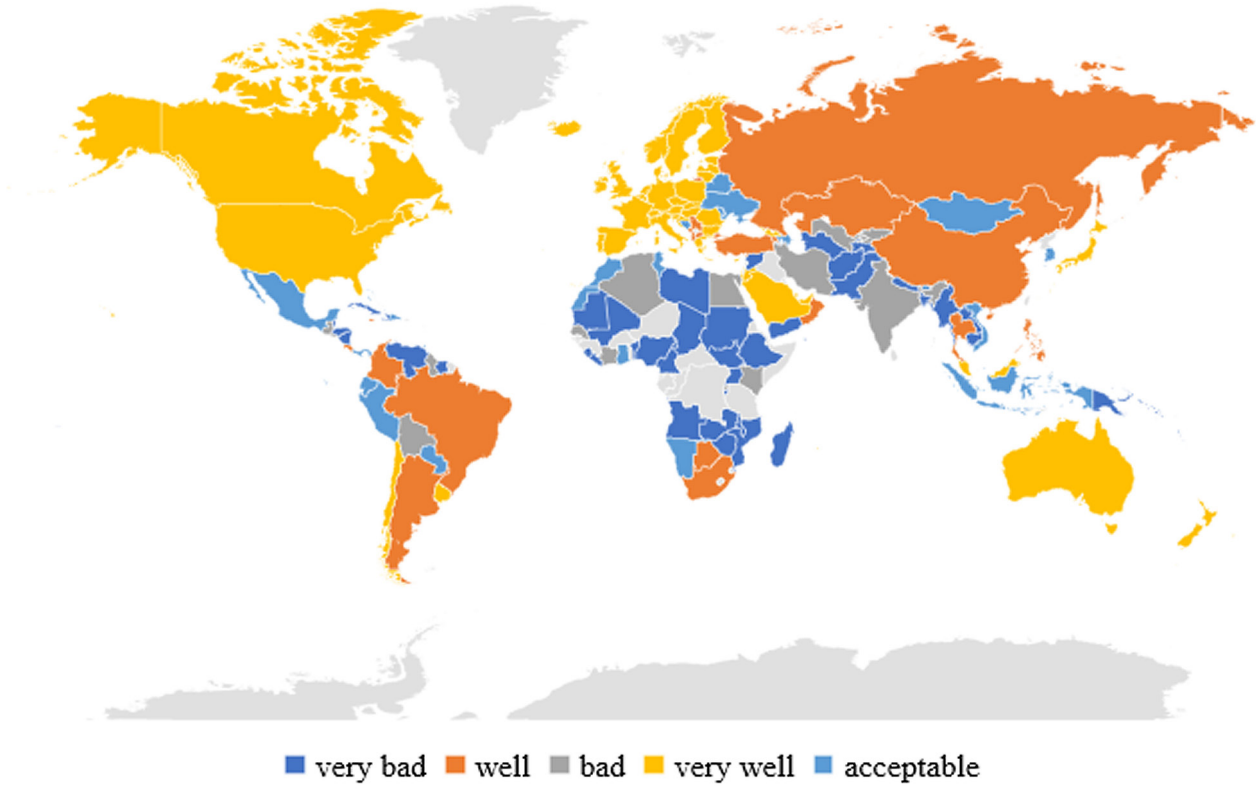

Figure 5. Map of the distribution of countries according to the information security threat index

sufficient economic potential, but their real information security indicators show deviations from the indicators of the "very well" group, especially for the National Cyber Security Index and ICT Development Index. Thus, the countries of this group need to change approaches to managing the country's information security system, improve cyber security standards, strengthen legal responsibility for cyber incidents, increase the level of protection of personal data of Internet and mobile users, and reform the institutions responsible for information security in the country.

The countries assigned to the "acceptable" group are 24 developing countries: Azerbaijan, Belarus, Moldova, Mongolia, Morocco, Peru, Tunisia, Ukraine, etc. This group is characterized by indicators of the country's development at the level of "well", but the level of information security is significantly lower than in the countries of the previous group. Therefore, in cases of situations associated with cyber terrorism, the countries of the "acceptable" group will be able to get out of the critical situation, but the consequences will significantly affect the social, economic, and political spheres. In contrast to the previous group, these countries should also develop a set of strategic measures that will contribute to the development of digital and computer technologies for information security. They can also include programs to improve the training level of cybersecurity specialists, make changes to security policies, legislative rules, introduce technologies to make decisions and prevent corruption in various areas, create plans for managing cyber crises, change approaches to protecting personal data, digital and computer services, etc. It is very important to create conditions associated with the organization of the listed activities and the ability to create long-term plans considering the latest achievements of the fourth industrial revolution to coordinate projects and startups in the IT field at the state level, and monitor their effectiveness.

The "bad" group includes 19 countries – Algeria, Barbados, Bolivia, Egypt, Guatemala, India, Iran, Uzbekistan, etc., the "very bad" group – 49 countries: Afghanistan, Cameroon, Cambodia, Libya, Mozambique, Nicaragua, Nigeria, Sudan, Tajikistan, Turkmenistan, etc. The countries of these groups are characterized by low or very low indicators of the country's development and the level of organization of information security. Accordingly, the risk of the information security threat to these countries is critical or significantly critical, i.e., they are more vulnerable. Their available economic resources are not sufficient to overcome the consequences of the cyber crisis, information terrorism, or information war. On the other hand, the risk that they will become the targets of cyber-terrorists is low compared to the countries of the "very well", "well", and "acceptable" groups. It can be assumed that the increase in the level of social and economic development of such countries will significantly affect measures aimed at increasing level of the country's information security. That is why the task of their development should become one of the main strategies for improving the state of information security.

The results of assessing the threat to information security based on the index can be considered adequate since the resulting groups of countries enlist states that are the same in the development category, which was demonstrated during the analysis of the results. The groups do not have a combination of countries that are fundamentally opposite in terms of the degree of development and information security level.

CONCLUSION

The results of the study led to several conclusions. The proposed assessment of the level of threat to the national information security takes into account not only individual areas, such as the level of cybersecurity, development of information technologies, the degree of digitalization and informatization, but also the level of development. The index's calculations enabled to form five groups of countries and carry out their qualitative identification and visualization in the form of a map of countries distributed by groups. In most cases, the "very well" group was formed by economically powerful countries with a high level of information security. The level of their resistance to threats is the highest one, indicating the significant capabilities of these countries to overcome the consequences of information wars and

http://dx.doi.org/10.21511/ppm.18(3).2020.17

threats. The "well" group includes new industrial countries and developing countries. Their level of resistance to threats suggests that these countries should improve their information security management strategy since there are some problems related to standardization, legal aspects, organization of information security institutions, etc. Developing countries with mediocre economic development indicators and the level of information security formed the "acceptable" group, which included Ukraine. Their level of resistance to information security threats indicates that the consequences of information threats will affect the economic, social, and political spheres. Therefore, these countries should reform the management strategy and develop programs to attract investment in the development and application of modern software and technological solutions in the field of information security. Countries with low socioeconomic development and low security and least developed countries are identified as "bad" and "very bad". These countries should solve tasks to improve the development level, which will stimulate an increase in the efficiency of the information security system.

The results obtained can be used to further predict the country's capabilities to withstand information threats and quickly overcome their consequences. The index's value will contribute to the development of information security management strategies and can be taken into account when forming the country's development plans. In the future, the proposed assessment can be improved by clustering countries and taking these results into account when justifying the groups' qualitative characteristics.

AUTHOR CONTRIBUTIONS

Conceptualization: Hanna Yarovenko.
Data curation: Hanna Yarovenko.
Formal analysis: Hanna Yarovenko.
Funding acquisition: Hanna Yarovenko.
Investigation: Hanna Yarovenko.
Methodology: Hanna Yarovenko.
Project administration: Hanna Yarovenko.
Resources: Hanna Yarovenko.
Software: Hanna Yarovenko.
Supervision: Hanna Yarovenko.
Validation: Hanna Yarovenko.
Visualization: Hanna Yarovenko.
Writing – original draft: Hanna Yarovenko.
Writing – review & editing: Hanna Yarovenko.

ACKNOWLEDGMENT

This work is carried out within the taxpayer-funded research: No. 0118U003574 "Cybersecurity in the banking fraud enforcement: protection of financial service consumers and the financial and economic security growth in Ukraine".

REFERENCES

1. Aldhous, P. (2020). *A Security Breach Exposed More Than One Million DNA Profiles On A Major Genealogy Database.* Retrieved from https://www.buzzfeednews.com/article/peteraldhous/hackers-gedmatch-dna-privacy
2. Anscombe, T. (2020). *Beware scams exploiting coronavirus fears.* Retrieved from https://www.welivesecurity.com/2020/03/13/beware-scams-exploiting-coronavirus-fears/
3. Bekmuratov, T. F., Ganiev, A. A., & Botirov, F. B. (2020). Concept of establishing multi-agent intellectual automatically systems in the enterprise. *International Journal of Scientific and Technology Research, 9*(4),

347-352. Retrieved from http://www.ijstr.org/paper-references.php?ref=IJSTR-0420-34436

4. Brožová, H., Šup, L., Rydval, J., Sadok, M., & Bednar, P. (2016). Information security management: ANP based approach for risk analysis and decision making. *Agris On-line Papers in Economics and Informatics, 8*(1), 13-23. Retrieved from https://ideas.repec.org/a/ags/aolpei/233959.html

5. Burke, W., Oseni, T., Jolfaei, A., & Gondal, I. (2019, January). Cybersecurity Indexes for eHealth. In *Proceedings of the 2019 Australasian Computer Science Week Multiconference, ACSW 2019 (Australia, Sydney, January, 2019), ACM International Conference Proceeding Series, Article No.: 17* (pp. 1-8). Retrieved from https://dl.acm.org/doi/10.1145/3290688.3290721

6. Cardholm, L. (2015). Identifying the business value of information security. In *Banking, Finance, and Accounting: Concepts, Methodologies, Tools, and Applications* (pp. 1056-1079). https://doi.org/10.4018/978-1-4666-6268-1.ch058

7. Deane, J. K., Goldberg, D. M., Rakes, T. R., & 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. https://doi.org/10.1007/s10799-018-00297-3

8. Dincelli, E. (2018). The role of national culture in shaping information security and privacy behaviors. In D. Siegel (Ed.), *World Scientific Reference on Innovation: Volume 4: Innovation in Information Security* (pp. 47-68). https://doi.org/10.1142/10209

9. Dorosh, M., Voitsekhovska, M., & Balchenko, I. (2019, January). Research and Determination of Personal Information Security Culture Level Using Fuzzy Logic Methods. In *Proceedings of the 2nd International Conference on Computer Science, Engineering and Education Applications, ICCSEEA 2019 (Ukraine, Kiev, 29 March 2019), Advances in Intelligent Systems and Computing, Volume 938* (pp. 503-512). https://doi.org/10.1007/978-3-030-16621-2_47

10. Dumas, E. (2020). *Mobile adware: The Silent Plague with No Origin.* Retrieved from https://www.cxotoday.com/news-analysis/mobile-adware-the-silent-plague-with-no-origin/

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

12. Frolova, E. E., Polyakova, T. A., Dudin, M. N., Rusakova, E. P., & 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. Retrieved from https://ideas.repec.org/a/srs/jarle0/v9y2018i1p89-95.html

13. Harrington, E. (1965). The Desirability Function. *Industrial Quality Control, 21, 10,* 494-498.

14. Jazri, H., Zakaria, O., & Chikohora, E. (2018, May). *Measuring cybersecurity wellness index of critical organisations.* Paper presented at 2018 IST-Africa Week Conference, IST-Africa 2018 (Botswana, Gaborone, May 2018), Institute of Electrical and Electronics Engineers Inc.

15. Kirilenko, V. P., & Alexeyev, G. V. (2018). Political technologies and international conflicts in the information space of the Baltic Sea region. *Baltic Region, 10*(4), 20-38. https://doi.org/10.5922/2079-8555-2018-4-2

16. Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in smes: Factors of success. *Entrepreneurship and Sustainability Issues, 6*(4), 2081-2094. https://doi.org/10.9770/jesi.2019.6.4(37)

17. Klyaus, T. K., & Gatchin, Yu. A. (2020, June). *Mathematical model for information security system effectiveness evaluation against advanced persistent threat attacks.* Paper presented at 2020 Wave Electronics and its Application in Information and Telecommunication Systems, WECONF 2020 (Russian Federation, Saint-Petersburg, 1-5 June 2020), Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/WECONF48837.2020.9131540

18. Kosevich, E. (2020). Estrategias de seguridad cibernética en los países de América Latina [Cyber security strategies of Latin America countries]. *Iberoamerica, 1,* 137-159. (In Spanish). https://doi.org/10.37656/S20768400-2020-1-07

19. Kshetri, N. (2017). An opinion on the 'Report on Securing and Growing the Digital Economy. *IEEE Security and Privacy, 15*(1), 80-85. https://doi.org/10.1109/MSP.2017.10

20. Mencher, Eh. M., & Zemshman, A. Ja. (1986). *Osnovy planirovaniya eksperimenta s elementami matematicheskoy statistiki v issledovanii po vinogradstvu [Basics of planning an experiment with elements of mathematical statistics in a study on viticulture].* Kishinev: Shtiintsa. (In Russian)

21. Morrow, S., & Crabtree, T. (2019). *The future of cybercrime & security. Threat Analysis, Impact Assessment & Mitigation Strategies 2019–2024.* Retrieved from https://www.juniperresearch.com/researchstore/key-vertical-markets/cybercrime-cybersecurity-research-report?utm_campaign=pr1_thefutureofcybercrime_technology_aug19&utm_source=businesswire&utm_medium=pr

22. Omirzhanov, Y., Baimagambetova, Z., Tusupova, A., Omirtay, R., & Uteuliev, S. (2017). On the national security correlation with freedom of speech in Kazakhstan. *Journal of Advanced Research in Law and Economics, 8*(3), 980-986. Retrieved from https://journals.aserspublishing.eu/jarle/article/view/1477

23. Park, S. (2019). Why information security law has been ineffective in

http://dx.doi.org/10.21511/ppm.18(3).2020.17

addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records. *International Review of Law and Economics, 58,* 132-145. https://doi.org/10.1016/j.irle.2019.03.007

24. Popova, L., Korostelkina, I., Dedkova, E., & Korostelkin, M. (2019, October). Information Risks and Threats of the Digital Economy of the XXI Century: Objective Prerequisites and Management Mechanisms. In T. Antipova & Á. Rocha (Eds.), *Digital Science 2019. DSIC 2019. Advances in Intelligent Systems and Computing, vol. 1114.* Springer, Cham. https://doi.org/10.1007/978-3-030-37737-3_17

25. Schmitz, C., & Pape, S. (2020). LiSRA: Lightweight Security Risk Assessment for decision support in information security. *Computers and Security, 90,* 101656. https://doi.org/10.1016/j.cose.2019.101656

26. Scopus. (2020). *Analyze search results.* Retrieved from https://www.scopus.com/term/analyzer.uri?sid=64b3d9ebe11f44b77acaf740b045aade&origin=resultslist&sr c=s&s=TITLE-ABS-KEY%28%22information+security%22+AND+%22economics%22%29&sort=plf-f&sdt=b&sot=b&sl=53&count=375&analyzeResults=Analyze+results&txGid=2c52702b

27. Singh, A. N., & Gupta, M. P. (2019). Information Security Management Practices: Case Studies from India. *Global Business Review, 20*(1), 253-271. https://doi.org/10.1177/0972150917721836

28. Sonny, Z. (2011). National security in Malaysia's digital economy: Redefinition, reaction and legal reform. *Journal of Applied Sciences Research, 7(special issue)*, 2316-2325. Retrieved from https://www.researchgate.net/publication/292497588_National_security_in_Malaysia's_digital_economy_Redefinition_reaction_and_legal_reform

29. StatSoft. (2020). *Produkty STATISTICA [STATISTICA products].* (In Russian). Retrieved from http://statsoft.ru/products/

30. The World Bank. (2020). *World Development Indicators.* Retrieved from https://databank.worldbank.org/source/world-development-indicators/Type/TABLE/preview/on

31. Topa, I., & Karyda, M. (2019). From theory to practice: guidelines for enhancing information security management. *Information and Computer Security, 27*(3), 326-342. https://doi.org/10.1108/ICS-09-2018-0108

32. VOSviewer. (2020). *Download VOSviewer.* Retrieved from https://www.vosviewer.com/download

33. Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management, 52,* 102090. https://doi.org/10.1016/j.ijinfomgt.2020.102090

34. Yunis, M. M., & Koong, K. S. (2015). *A conceptual model for the development of a national cybersecurity index: An integrated framework*. Paper presented at 21st Americas Conference on Information Systems, AMCIS 2015 (Puerto Rico,El Conquistador Resort and Convention Center Fajardo). Retrieved from https://aisel.aisnet.org/amcis2015/ISSecurity/GeneralPresentations/44/

APPENDIX A

Table 1A. World Development Indicators

ID	Indicator name
1	GDP per capita (current USD)
2	General government final consumption expenditure (% of GDP)
3	Portfolio investment, net (BoP, current USD)
4	Unemployment, total (% of total labor force) (modeled ILO estimate)
5	Life expectancy at birth, total (years)
6	Total reserves (includes gold, current USD)
7	Current account balance (% of GDP)
8	Wage and salaried workers, total (% of total employment) (modeled ILO estimate)
9	GINI index (World Bank estimate)
10	Control of corruption: estimate
11	Government effectiveness: estimate
12	Political stability and absence of violence/terrorism: estimate
13	Regulatory quality: estimate
14	Rule of law: estimate
15	Exports of goods and services (% of GDP)
16	External debt stocks, total (DOD, current USD)
17	Foreign direct investment, net inflows (BoP, current USD)
18	GDP (current USD)
19	GDP growth (annual %)
20	GNI per capita, PPP (current international USD)
21	GNI, PPP (current international USD)
22	Gross capital formation (% of GDP)
23	Imports of goods and services (% of GDP)
24	Industry (including construction), value added (% of GDP)
25	Inflation, GDP deflator (annual %)
26	Mobile cellular subscriptions (per 100 people)
27	Revenue, excluding grants (% of GDP)
28	Statistical capacity score (overall average)
29	Tax revenue (% of GDP)
30	Individuals using the Internet (% of population)
31	Secure Internet servers (per 1 million people)
32	Charges for the use of intellectual property, payments (BoP, current USD)
33	Charges for the use of intellectual property, receipts (BoP, current USD)
34	High-technology exports (% of manufactured exports)
35	Patent applications, nonresidents
36	Patent applications, residents
37	Scientific and technical journal articles

http://dx.doi.org/10.21511/ppm.18(3).2020.17