



## Cyber Security in Terms of Ensuring the Digital Transformation of European Economies: Empirical Evidence

Vasyl Hyk<sup>\*1</sup>, Oleh Vysochan<sup>2</sup>, Olha Vysochan<sup>3</sup>

---

### Abstract

The development of information technologies actualizes the issue of ensuring information and cyber security, while the main problem can be considered the lack of a clear understanding of the key role of cyber security in strengthening the national security of the state. The purpose of the article is to identify the interdependence between the cyber security system in the country and opportunities for using modern digital technologies in economic processes, which can ultimately accelerate the digital transformation of the economy. This study used a basic model for linear regression between the National Cyber Security Index and Digital Development Level indicators. The results of the study showed an average level of the close relationship between the studied indicators, and the value of the multiple correlation coefficient in the total number of observations of equal 37 studied European countries is 0.46445. As a result of the positioning between the effective and factor indicators, we identified 4 zones (groups) of countries and established that their distribution according to economic similarity is preserved, the essence of which boils down to the fact that the countries have similar geographical conditions and implement similar strategies of economic development and digital transformation.

### Keywords

Digital Economy, Cyber Security, National Cyber Security Index, Information Security, Risk

---

### I. Introduction

The digital economy is the modern driver of socio-economic development, gaining competitiveness and improving the quality of life both for a single country and the whole world. The development of the digital economy in the modern world is aimed at the creation and

---

\* Corresponding author

<sup>1</sup> Lviv Polytechnic National University, Stepan Bandera Str. 12, 79013 Lviv, Ukraine.  
E-mail: vasyi.v.hyk@lpnu.ua.

<sup>2</sup> Lviv Polytechnic National University, Stepan Bandera Str. 12, 79013 Lviv, Ukraine.  
E-mail: oleh.s.vysochan@lpnu.ua.

<sup>3</sup> Lviv Polytechnic National University, Stepan Bandera Str. 12, 79013 Lviv, Ukraine.  
E-mail: olha.o.vysochan@lpnu.ua.

unification of a communicative society, ensuring the social growth of information platforms and startups, the conversion of financial infrastructure, the acceleration of monetary transactions, the digitization of administrative and civil services, etc. In connection with the development of the information society, digital transformation, and technologies, the state faces the task of finding opportunities to regulate such phenomena as robotics and cyber systems, artificial intelligence, Big Data, the Internet of Things, Internet banking, information, and educational platforms, blockchain, unmanned and mobile technologies, etc. Digitalization processes are rapidly spreading and gaining special significance in all spheres of life, at the same time generating new threats and challenges, opening up previously unknown opportunities for abuse and legal violations. For these reasons, the complex issue of developing and implementing effective measures to combat cybercrime has arisen globally. Its solution requires a systematic and complex approach because the digital economy is built on a wide list of key digital technologies and infrastructure, the applied implementation of which in one or another area forms and expands the contours of the digital environment, along with providing new functionality, increasing risks.

The ISO / IEC 27032 standard defines cyber security as a type of security in an interactive information environment, which makes it possible to preserve the confidentiality, integrity, and availability of information in a virtual environment. In this case, cyberspace is the result of functioning based on general principles and rules of information and communication systems (ISO/IEC 27032:2012). According to DSTU ISO/IEC 27032:2016, cyberspace is a complex interactive information environment that arises and functions as a result of the cooperation of people, computer systems, and Internet services and operates thanks to integrated networks and technical equipment (DSTU ISO/IEC 27032:2016). Unlike information security, cyber security is not only about protecting cyberspace itself but also about protecting those who operate in cyberspace and any of their assets that can be accessed through cyberspace. Cyber security is the protection of information assets by eliminating threats to information processed, stored, and transmitted between networked information systems. Cybersecurity is a complex concept that combines in its essence the objective basis of cyberspace and the procedural functionality of the protection mechanism, is based on systemic and institutional approaches, and the principles of efficiency, reliability, and optimality.

The digital economy is changing social life, and its innovativeness opens up new opportunities not only for the country's economic growth, business competitiveness, public welfare, and the quality of life of individual citizens but also creates new motives and types of cyber threats and illegal activities.

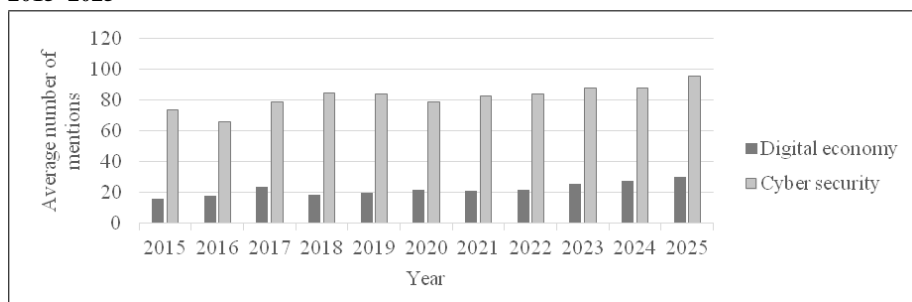
All the countries of the world are exposed to threats, without exception, and the problem of cyber security is becoming very acute and important. It follows that the further development of the digital economy and humanity's receipt of its benefits is inextricably linked with the simultaneous development of relevant cybersecurity systems (Kindzerskyi, 2020; Vysochan et al., 2021).

## II. Literature Review and Hypotheses Development

Building a digital economy is impossible without understanding the technological and social nature of cyber threats and requires initiatives and effective steps to develop and strengthen institutional and information infrastructure at the national and global levels, develop a reliable and consistent legal framework, and develop the necessary digital competencies and digital literacy, including regarding models of cyber threats and mechanisms of cybercrimes and their consequences, compliance with the principles of cyber security in all spheres of professional activity and the construction of smart-oriented ecosystems, etc.

The most popular Google search engine was used to study the frequency of queries for the terms Cyber security and Digital economy. Using Google as a search engine makes it expedient to use the Google Trends Internet service as a research tool. The main purpose of conducting data analysis using the Google Trends application and comparing search queries was to identify the general level of awareness and interest in this field in the world. Google Trends allows you to get data on the popularity and seasonality of certain search queries, evaluate the influence of geographic data on the frequency of their appearance, etc. A graphic representation of the trend of the frequency of appearance of the term Cyber security and Digital economy is shown in Fig. 1.

**Figure 1: Search results in Google Trends by keyword Cyber security and Digital economy for 2015–2025**



Source: Google Trend (2025)

According to the given data, it can be seen that the term cyber security has become increasingly popular in recent years. At that time, the use of the term Digital economy is less popular but remains consistently average. The obtained results indicate that a significant number of the target audience is looking for information. The above actualizes the need for further research in the field of cyber security to ensure the digital transformation of the economy.

The scientific works of many researchers highlight the issues of monitoring digital processes, identifying threats to information and cyber security, and protecting the information space from cyber attacks and cyber terrorism. In particular, the works are devoted to these issues of Blikhar et al. (2023), Hyk (2021), Kindzerskyi (2020), Kuzior et al. (2022), Mat et al. (2019), Möller (2023), Nehrey and Zomchak (2022), Peng (2023), Pizhuk (2020), Revak

and Gren (2021), Shpak et al. (2021), Teoh and Mahmood (2017), Verma et al. (2021), Vysochan et al. (2023), Yerina et al., 2021, etc. Separate studies touch on issues of the digital economy, the development of digital technologies, and infrastructure. In particular, they reveal the importance of cyber security in the formation of the digital economy (Kindzerskyi (2020); Mat et al. (2019); Pizhuk (2020), Revak and Gren (2021)); the level of readiness of countries to protect data in cyberspace according to the Global Cybersecurity Index (GCI) and National Cyber Security Index (NCSI) was analyzed (Kindzerskyi (2020); Pizhuk (2020)); the challenges of the digital economy are considered in the context of cyber security threats that have implications for national security (Peng, 2023); the relationship between the development of the National cybersecurity strategy (NCSS) and the success of the country's digital economy was analyzed (Teoh and Mahmood (2017)); the relationship between the digital and green economy was identified, and the ways of environmentally safe development of digital technologies were substantiated (Yerina et al., 2021; Hyk et al., 2021).

It is worth noting that in some scientific works, the authors used mathematical tools and provided models to explain the connection between cyber security and the digital economy. Thus, in their work, Kuzior et al. (2022) investigated the impact of cyber security, business transparency, and economic transformation measures to ensure Global Digital Convergence. The econometric model proposed by the authors describes the impact of statistically significant integral indicators of the level of national cyber security, ease of doing business, and the anti-money laundering index on the level of digital development of the country. The results of the data analysis of 104 countries made it possible to determine the average trend of dependence on the level of digital development.

However, their research is mostly focused on the field of legal regulation and the formation of the information security system, while at the same time, the impact of cyber security on the processes of digital transformation of the economy remains insufficiently studied.

Considering the above, we proposed a research hypothesis that assumes that ensuring security in cyberspace will contribute to increasing the level of digital development in countries.

### **III. Methodology and Data Analysis**

The National Cyber Security Index and Digital Development Level data were used as the source of information for the research.

The National Cyber Security Index is a global index that measures countries' preparedness to prevent cyber threats and respond to incidents. Among the criteria taken into account when calculating the index is the state's ability to identify threats, the creation of security systems, and the development of education in the field of cybersecurity. When calculating the rating, they analyze, in particular: legislation in the field of cyber security, cyber incidents; education in the field of cyber security; ensuring the protection of services, in particular, electronic services; electronic identification and trust services; protection of personal data; measures to respond to cyber attacks and cyber incidents; fight against cybercrime (National Cyber Security Index 2022).

The Digital Development Level (DDL) is calculated as the average percentage that the country received from the maximum value of both indices, according to the ICT Development Index (IDI) and Networked Readiness Index (NRI) according to the formula:

$$DDL = \frac{IDI, \% + NRI, \%}{2} \quad (1)$$

In turn, the ICT Development Index (IDI) is the most famous index that characterizes the level of development of the information society of countries. This comprehensive indicator includes 11 items grouped into 3 sub-indices: access to ICT, use of ICT, and skills in the field of ICT.

The Networked Readiness Index (NRI) is an index published annually by the World Economic Forum in collaboration with INSEAD since 2002 as part of the annual report on global information technologies. This index is aimed at measuring the degree of readiness of the countries of the world to use the opportunities opened by information and information and communication technologies. It includes metrics grouped into 4 categories: technology, users, governance, and impact.

As a result, in Table 1, we will present grouped information on the National Cyber Security Index and Digital Development Level indicators.

It is possible to quantitatively assess the relationship and interdependence between indicators (characteristics) based on statistical methods. Indicators that characterize the cause are called factors (independent, exogenous). Accordingly, effective (dependent) indicators are those that characterize the consequence (result) of the change. A set of factor and result indicators connected by a certain dependence is called a factor system. Multiple linear regression is a generalization of linear regression taking into account more than one independent variable, and a special case of the general linear model is formed by limiting the number of dependent variables to one. The basic model for linear regression is:

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \dots + \beta_n x_n + \varepsilon \quad (2)$$

where,  $y$  – the dependent variable of the model,  $x_1, x_2, \dots, x_n$  – independent variable models or factors,  $\beta_0, \beta_1, \beta_2, \dots, \beta_n$  – model parameters (regression coefficients),  $\varepsilon$  – stochastic component model,  $n$  – the number of explanatory variables in the model.

This model was successfully tested in our previous studies (Hyk et al., 2022). In our case, the formula will be slightly different and will look like this:

$$y = \beta_0 + \beta_1 x + \varepsilon \quad (3)$$

where,  $y$  – Digital Development Level,  $x$  – National Cyber Security Index.

**Table 1: Rating of European countries by indicators National Cyber Security Index and Digital Development Level**

| Country                | National Cyber Security Index (Score/Value) | National Cyber Security Index rank (1–176 place) | Digital Development Level (Score/Value) | Digital Development Level rank (1–176 place) |
|------------------------|---------------------------------------------|--------------------------------------------------|-----------------------------------------|----------------------------------------------|
| Albania                | 62,34                                       | 51                                               | 48,74                                   | 85                                           |
| Austria                | 85,71                                       | 12                                               | 75,76                                   | 19                                           |
| Belgium                | 94,81                                       | 1                                                | 74,07                                   | 23                                           |
| Bosnia and Herzegovina | 28,57                                       | 112                                              | 49,31                                   | 82                                           |
| Bulgaria               | 74,03                                       | 28                                               | 62,06                                   | 52                                           |
| Croatia                | 83,12                                       | 18                                               | 64,63                                   | 43                                           |
| Cyprus                 | 66,23                                       | 39                                               | 68,83                                   | 31                                           |
| Czech Republic         | 92,21                                       | 4                                                | 69,21                                   | 29                                           |
| Denmark                | 84,42                                       | 17                                               | 82,68                                   | 2                                            |
| Estonia                | 93,51                                       | 3                                                | 75,59                                   | 20                                           |
| Finland                | 85,71                                       | 13                                               | 78,35                                   | 14                                           |
| France                 | 84,42                                       | 15                                               | 77,29                                   | 16                                           |
| Germany                | 90,91                                       | 5                                                | 80,01                                   | 8                                            |
| Greece                 | 89,61                                       | 7                                                | 64,02                                   | 45                                           |
| Hungary                | 67,53                                       | 36                                               | 64,25                                   | 44                                           |
| Iceland                | 55,84                                       | 64                                               | 78,64                                   | 12                                           |
| Ireland                | 75,32                                       | 26                                               | 75,18                                   | 22                                           |
| Italy                  | 79,22                                       | 23                                               | 67,26                                   | 35                                           |
| Latvia                 | 75,32                                       | 25                                               | 66,23                                   | 36                                           |
| Lithuania              | 93,51                                       | 2                                                | 67,34                                   | 34                                           |
| Luxembourg             | 66,23                                       | 41                                               | 78,4                                    | 13                                           |
| Malta                  | 50,65                                       | 76                                               | 71,74                                   | 27                                           |
| Montenegro             | 35,06                                       | 95                                               | 57,79                                   | 63                                           |
| Netherlands            | 83,12                                       | 20                                               | 81,86                                   | 4                                            |
| North Macedonia        | 58,44                                       | 58                                               | 55,36                                   | 70                                           |
| Norway                 | 67,53                                       | 38                                               | 80,19                                   | 7                                            |
| Poland                 | 87,01                                       | 11                                               | 65,03                                   | 41                                           |
| Portugal               | 89,61                                       | 8                                                | 68,46                                   | 32                                           |
| Romania                | 89,61                                       | 6                                                | 59,84                                   | 56                                           |
| Serbia                 | 80,52                                       | 21                                               | 59,81                                   | 57                                           |
| Slovak Republic        | 83,12                                       | 19                                               | 65,44                                   | 37                                           |
| Slovenia               | 59,74                                       | 56                                               | 69,74                                   | 28                                           |
| Spain                  | 88,31                                       | 10                                               | 72,21                                   | 26                                           |
| Sweden                 | 84,42                                       | 16                                               | 81,51                                   | 5                                            |
| Switzerland            | 75,32                                       | 27                                               | 82,93                                   | 1                                            |
| Ukraine                | 75,32                                       | 24                                               | 55,96                                   | 68                                           |
| United Kingdom         | 89,61                                       | 9                                                | 79,96                                   | 9                                            |

*Source: National Cyber Security Index (2022)*

In our study, the interdependence between the two indicators National Cyber Security Index and Digital Development Level is established using the Pearson correlation coefficient. The Pearson correlation coefficient (Pearson correlation coefficient, pairwise correlation coefficient, sample correlation coefficient, Bravais-Pearson coefficient) measures the degree of linear correlation between quantitative scalar features (Pearson's correlation). The coefficient is calculated according to the formula:

$$r_{xy} = \frac{\sum_{i=1}^m (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^m (x_i - \bar{x})^2 \sum_{i=1}^m (y_i - \bar{y})^2}} = \frac{\text{cov}(x, y)}{\sqrt{s_x^2 s_y^2}} \quad (4)$$

where,  $\bar{x}, \bar{y}$  – sample means  $x^m$  i  $y^m$ ,  $s_x^2, s_y^2$  – sample variances,  $r_{xy}$  takes values in the interval  $-1 \leq r_{xy} \leq +1$ . For the verbal description of the value of the correlation coefficient, the following gradations are used, which are given in the table 2.

**Table 2: The value of the correlation coefficient**

| Interpretation | very weak     | weak            | average         | high            | very high     |
|----------------|---------------|-----------------|-----------------|-----------------|---------------|
| Value (modulo) | from 0 to 0,1 | from 0,1 to 0,4 | from 0,4 to 0,7 | from 0,7 to 0,9 | from 0,9 to 1 |

Source: Formed by the authors

The strength of the connection does not depend on its direction and is determined by the absolute value of the correlation coefficient. If the modulus correlation coefficient is close to 1, then this corresponds to a high level of connection between the variables.

Using the data of Table 1, using the “Data Analysis” package of the MS Excel software, a factorial model of dependence between variables was formed.

## IV. Results

Analyzing the position of countries according to the National Cyber Security Index, it should be noted that Belgium became the leader of the rating with the value of the indicator of 94.81 points. Lithuania is on the second step of the rating with an estimate of 93.51 points, and Estonia is in third place with 93.51 points. According to the data, Ukraine took 24th place with a score of 75.32 points, ahead of such highly developed countries as Switzerland (75.32 points), Hungary (67.53 points), and Norway (67.53 points). The strengths of our country were noted for the achievements in the field of implementation of cyber security policy, protection of personal data, and fight against cybercrime. Among the weak ones should be noted the positions on the management of incidents and cyber crises, as well as the protection of electronic services, analysis, and informing the public about cyber threats. The increase in Ukraine's position in the rating is due to the effective work of the CERT-UA computer emergency response team, which works in close cooperation with the Cisco Talos Intelligence Group and other CERT member states on issues of overcoming the consequences of cyber attacks on critical information infrastructure and identifying the causes and circumstances of such incidents. CERT-UA also helps to eliminate security threats to the private sector of Ukraine and foreign partners. By the law “On the basic

principles of ensuring cyber security of Ukraine” (Law of Ukraine, 2017), adopted in 2017, CERT-UA and the Cybercrime Response Center coordinate the measures of operational response to cyber attacks, as well as monitor the implementation of countermeasures that involve minimizing the vulnerability of systems connection Ukraine participates in the work of the EU Agency for Cyber Security, the European Center for Research and Competence in Cyber Security, as well as in exercises to implement the Joint Operational Response Scheme of the EU and its member states to cyber attacks (Pizhuk, 2020).

According to the Digital Development Level, the main players of the information technology market in the context of globalization are European countries – Switzerland, Denmark, the Netherlands, and Sweden, whose economies have a high level of digital development. According to the rating, Ukraine took 68th place out of 176. Among the reasons for Ukraine’s low place in the rating, the uneven development and implementation of ICT in various spheres of life and individual regions is the most significant.

Since the general assumption of our work is the hypothesis that ensuring security in cyberspace will contribute to increasing the level of digital development in countries, we used the method of correlation-regression modeling, which made it possible to establish a close relationship between the National Cyber Security Index and Digital Development Level (Table 3).

**Table 3: The results of regression statistics across European countries**

| Regression Statistics |             |
|-----------------------|-------------|
| Multiple R            | 0,464452314 |
| R Square              | 0,215715952 |
| Adjusted R Square     | 0,195076898 |
| Standard Error        | 8,439918414 |
| Observations          | 37          |

*Source: Calculated by the authors*

The value of the multiple correlation coefficient in the total number of observations of 37 European countries under study is 0.46445, which indicates the average closeness of the connection between the data arrays (Chaddock scale). The coefficient of determination (R-squared) is 0.21571%. This means that the estimated parameters of the model explain the dependence between the proposed indicators by almost 22%, also demonstrating the average relationship between the variables. The value of R square, the value of which is  $< 0.4$ , confirms that the accuracy of the approximation is insufficient, and the model requires the introduction of new independent variables.

In table 4 we will present the results of the analysis of variance (ANOVA), which is a statistical method of analyzing results that depend on qualitative characteristics.

**Table 4: Results of dispersion analysis**

|                                                                               | df           | SS             | MS          | F           | Significance F |
|-------------------------------------------------------------------------------|--------------|----------------|-------------|-------------|----------------|
| Regression                                                                    | 1            | 744,5073       | 744,5073    | 10,45183    | 0,002534987    |
| Residual                                                                      | 38           | 2706,824       | 71,23222    |             |                |
| Total                                                                         | 39           | 3451,332       |             |             |                |
| Description of the confirmation of the hypothesis regarding the observed data |              |                |             |             |                |
|                                                                               | Coefficients | Standard Error | t Stat      | P-value     |                |
| Intercept                                                                     | 49,66064058  | 6,172664       | 8,045253    | 9,93755E-10 |                |
| X Variable 1                                                                  | 0,260462864  | 0,080566       | 3,23293     | 0,002534987 |                |
| Description with 95% probability                                              |              |                |             |             |                |
| Lower 95%                                                                     | Upper 95%    | Lower 95,0%    | Upper 95,0% |             |                |
| 37,16473565                                                                   | 62,15655     | 37,16474       | 62,15655    |             |                |
| 0,097366361                                                                   | 0,423559     | 0,097366       | 0,423559    |             |                |

Source: Calculated by the authors

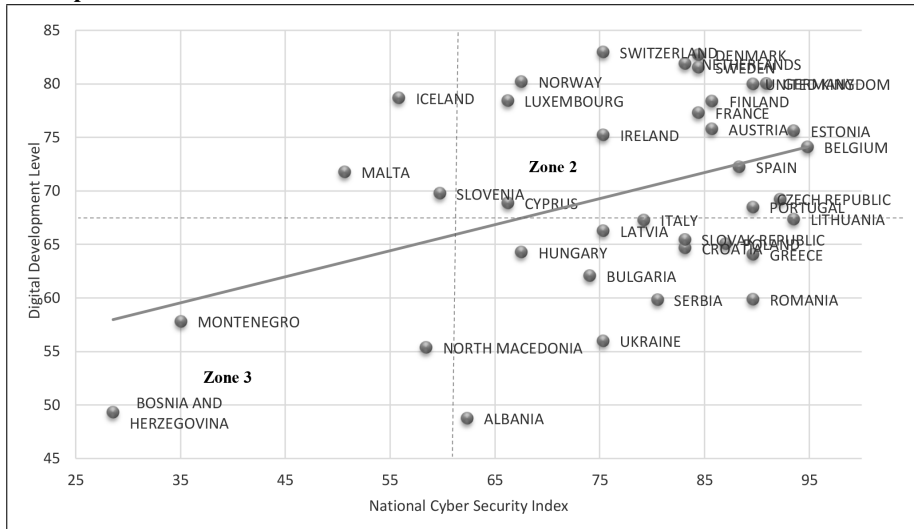
Fisher's exact test is used to test for equality of variances between two samples. The F-test (significance coefficient or F-statistic) is used in statistics to test the significance of a regression model by comparing the variance explained by the model to the variance of the error. A high value relative to the critical value (or low p-value) indicates that the model is statistically significant. Since the actual value of Fisher's ratio (10.45183) is greater than the critical value (0.002534987) with a probability of 95%, that is, we can conclude that ensuring security in cyberspace will contribute to increasing the level of digital development in countries.

As a result, the regression equation will look like this:

$$y = 0,2605x + 49,6606 \quad (5)$$

According to the obtained regression equation, if the National Cyber Security Index reaches a value of 10, the National Cyber Security Index will reach a value of more than 52. We are using the information in the table 1, we will conduct clustering (Vysochan et al., 2022) and visually present the place of each of the studied European countries in the coordinate system according to the level of cyber security (X-axis) and the level of digital transformation of the economy (Y-axis) (Fig. 2).

**Figure 2: Positioning of European countries by National Cyber Security Index and Digital Development Level**



Source: Calculated by the authors

Based on the obtained data on the positioning between effective and factor indicators, we selected 4 zones (groups) of countries (Table 5).

**Table 5: Results of zoning of countries**

| Characteristics of the zone                                                                            | Countries                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (Zone 1) Countries with a high level of digital development and a low level of cyber security          | Iceland, Malta, Slovenia                                                                                                                                                                                       |
| (Zone 2) Countries with a high level of digital development and a high level of security in cyberspace | Ireland, Spain, Portugal, Poland, Estonia, Czech Republic, Cyprus, Denmark, Sweden, Finland, Austria, France, United Kingdom, Norway, Germany, Netherlands, Belgium, Switzerland, Italy, Luxembourg, Lithuania |
| (Zone 3) Countries with a low level of digital development and a low level of cyber security           | Montenegro, Bosnia and Herzegovina, North Macedonia                                                                                                                                                            |
| (Zone 4) Countries with a low level of digital development and a high level of cyber security          | Albania, Ukraine, Serbia, Romania, Hungary, Bulgaria, Croatia, Greece, Latvia, Slovak Republic                                                                                                                 |

Source: Calculated by the authors

Zone 1 is represented by countries with a high level of digital development with a low level of security in cyberspace. Among the studied European countries, this zone includes only 3 countries: Iceland, Malta, and Slovenia.

Zone 2 included the largest number of countries, namely: Ireland, Spain, Portugal, Poland, Estonia, Czech Republic, Cyprus, Denmark, Sweden, Finland, Austria, France, United Kingdom, Norway, Germany, Netherlands, Belgium, Switzerland, Italy, Luxembourg, Lithuania. These are highly developed countries in the world, both in terms of digital development and in the field of cyber security. The entry of most countries into this zone somewhat confirms our assumption and indicates that there is a connection between the levels of cyber security and the digital development of the economy.

Zone 3, like Zone 1, includes only three countries: Montenegro, Bosnia and Herzegovina, and North Macedonia.

Zone 4 is represented by countries that had a high status in cyber security at the same time as a low level of digital development. In this zone was Ukraine, which demonstrated weak positions in the rating by the level of digital development.

As a result of the analysis, it can be stated that the distribution of countries according to economic similarity remains, the essence of which boils down to the fact that countries have similar geographical conditions and implement similar strategies of economic development and digital transformation. A comparison of the two rankings of cyber security and digital development in countries shows that they show an average level of connection between the two. That is, increasing the level of cyber security is not always sufficient to ensure the development of the digital economy.

The results of the study confirm that effective cybersecurity in the digital age requires a transition from reactive protection to proactive resilience management. One of the major challenges on the path of countries to digital transformation is the need to create a high level of information security, which is not always feasible for most of them (Kliuchnyk et al., 2025; Dvouletý et al., 2025). At the same time, the human factor remains important, since without personnel training and the formation of a digital culture, even the most advanced security systems will be ineffective. Governments need to develop their own “digital security roadmaps” that take into account industry specifics, size, geography and level of digital maturity (Petrová, 2022). Thus, it can be argued that in modern conditions, cybersecurity is not just about protecting against threats, but about the ability to generate sustainable value in the context of constant digital transformation. Only a comprehensive, flexible and people-oriented approach will ensure the development of the state in the new digital reality.

Summarizing, it can be assumed that to ensure information security in the economy with the advent of global digitalization, the following measures are taken:

- \* additional support for business entities in creating digital technologies, platforms and providing digital services;
- \* increasing the volume of training for IT specialists;
- \* formation of industry, regional and national cybersecurity systems (Hryshchenko et al., 2025). In particular, it is necessary to improve legislation on combating cybercrime, create protection units in law enforcement agencies, develop secure technological solutions, and ensure the interaction of all participants in the global digital economy. However, it should be remembered that security should not hinder the growth and

development of technologies. It is also necessary to strengthen the exchange of information between countries in the field of cybersecurity.

## **V. Conclusion**

The development of the digital economy is impossible without strengthening cyber security both at the state level and at the level of individual entities. With the help of correlation-regression analysis of factors, it was possible to establish the influence of factors, determine their correlation characteristics, form models, and carry out a statistical assessment of communication parameters. The proposed sample from 37 European countries is sufficiently large and representative. The results of the analysis show that there is a moderately close relationship between the levels of cyber security and digital development.

Based on the data of the cluster analysis, 4 groups of countries are distinguished: Zone 1 – Countries with a high level of digital development and a low level of security in cyberspace; Zone 2 – Countries with a high level of digital development and a high level of security in cyberspace, Zone 3 – Countries with a low level of digital development and a low level of security in cyberspace and Zone 4 – Countries with a low level of digital development and a high level of security in cyberspace. It is worth noting that in the group of the most developed countries, the relationship between indicators is best expressed. This confirms the fact that attention should be paid to balanced development both in the processes of cyber security and in the field of digitalization. The state, together with business, should make efforts to develop and implement effective cyber security systems of state and corporate management, conduct scientific research on the development of cyber protection tools in legal, organizational, and technical aspects, and start information and training campaigns to increase awareness and skills in the field of cyber security for civil servants, company personnel, ordinary citizens. At the same time, it should be taken into account that increasing the level of cyber security by itself is not always sufficient to ensure the development of the digital economy since it depends on other factors, such as the general level of economic, technological, and social development of the country, its position in the world economy, the effectiveness of the state management, level of protection of property rights. The latter should be an upward trend in the formation of the state cyber security strategy and the further development of the digital economy, since all cybercrimes, without exception, are associated with the unauthorized redistribution of these rights. For Ukraine, their protection is a problem because the state, due to its institutional features, is itself quite often the main violator of these rights both for businesses and citizens, and cybercrimes often become only a tool in the hands of the authorities in the illegal redistribution of property through the use of modern information and communication technologies.

The conducted research has certain limitations that should be taken into account during their interpretation and practical application. First, the theoretical conclusions are based mainly on the analysis of available scientific sources and the generalization of practices, which limits the possibility of fully taking into account the specifics of individual industries and regional features of digital transformation. Second, the time constraints that related to the use of data for a certain period of time. Third, the model contains only one explanatory

variable, and the obtained empirical results require additional research to confirm their effectiveness and universality.

A further direction of research may include a detailed analysis of the causes and consequences of preventing cyber threats. Promising directions for further research are a deeper analysis of the factors that determine cybersecurity in the context of digital transformation of the economy. It is also advisable to direct future scientific research to empirical testing in different sectors of the economy.

## References

- Blikhar, M., Syrovatskyi, V., Bek, U., Vinichuk, M., Kucher, L., Kashchuk, M. (2023). Shadow Economy vs Economic Security: Trends, Challenges, Prospects. *Economic Studies (Ikonomicheski Izsledvania)*, 32(3), 130–147.
- DSTU ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) (2016), “Information technologies. Methods of protection. Cybersecurity Guidelines”, no. 448. Available at [http://online.budstandart.com/ua/catalog/doc-page.html?id\\_doc=69128](http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69128).
- Dvoutely, O., Jirásek, M., Giglio, C., Liguori, E. (2025). Artificial intelligence, digitalization, and new technologies in shaping business and management research. *Cogent Business & Management*, 12(1), 2580126. <https://doi.org/10.1080/23311975.2025.2580126>.
- Google Trend. (2025). Retrieved from <https://trends.google.com/trends/explore?cat=12&date=2025-01-01%202025-12-31&q=cyber%20security,%2Fm%2F02plw6y&hl=en-GB>.
- Hryshchenko, S., Savchenko, V., Kumeiko, A., Patsuriia, N., Rieznikova, V. (2025). Current State of Information Security in Ukraine. *Danube*, 16(1), 16–29. <https://doi.org/10.2478/danb-2025-0002>.
- Hyk, V. (2021). Optimization of costs for innovations of industrial enterprises Western Ukraine in ensuring sustainable environmental development. *E3S Web of Conferences*, 234, 00049. <https://doi.org/10.1051/e3sconf/202123400049>.
- Hyk, V., Vysochan, O., Vysochan, O. (2021). Modeling the options for accounting for the innovation costs of industrial enterprises in Ukraine. *Intellectual economics*, 15(1), 88–103. <https://doi.org/10.13165/IE-21-15-1-06>.
- Hyk, V., Vysochan, O., Vysochan, O. (2022). Analysis of the relationship between the state of cluster development and sustainable growth: evidence from European countries. *Eastern Journal of European Studies*, 13(2), 246–262. <https://doi.org/10.47743/ejes-2022-0212>.
- ISO/IEC 27032:2012 “Information technology – Security techniques – Guidelines for cybersecurity”. Available at: [www.iso.org/standard/44375.html](http://www.iso.org/standard/44375.html). (access date March 06, 2023).
- Kindzerskyi, Yu. V. (2020). Cybersecurity and becoming of the digital economy: problems of interconnection. *Economics Bulletin*, 3, 18–26. <https://doi.org/10.33271/ebdut/71.018>.

Kliuchnyk, A., Shyshpanova, N., Sokolik, V., Ostapenko, A., Kryvko, O. (2025). Digitalisation of Public Administration Processes in Shaping the Investment Environment of Territorial Communities. *Danube*, 16(3), 264–276. <https://doi.org/10.2478/danb-2025-0013>.

Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., Brožek, P. (2022). Global Digital Convergence: Impact of Cybersecurity, Business Transparency, Economic Transformation, and AML Efficiency. *Journal of Open Innovation: Technology, Market, and Complexity*, 8, 195. <https://doi.org/10.3390/joitmc8040195>.

Law of Ukraine “About the main ambush of cyber security in Ukraine” (2017). Retrieved from <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.

Mat, B., Pero, S., Wahid, R., Sule, B. (2019). Cybersecurity and Digital Economy in Malaysia: Trusted Law for Customer and Enterprise Protection. *International Journal of Innovative Technology and Exploring Engineering*, 8(8S3), 214–220.

Möller, D. P. F. (2023). Cybersecurity in Digital Transformation. In Guide to Cybersecurity in Digital Transformation. *Advances in Information Security*, 103. Springer, Cham. [https://doi.org/10.1007/978-3-031-26845-8\\_1](https://doi.org/10.1007/978-3-031-26845-8_1).

National Cyber Security Index. (2022). Retrieved from <https://www.security-risks.com/post/national-cyber-security-index-2022>.

National Cyber Security Index. (2022). Retrieved from <https://ncsi.ega.ee/ncsi-index/?order=name>.

Nehrey, M., Zomchak, L. (2022). Digital Technology: Emerging Issue for Agriculture. Lecture Notes on Data Engineering and Communications Technologies, 135, 146–156. [https://doi.org/10.1007/978-3-031-04809-8\\_13](https://doi.org/10.1007/978-3-031-04809-8_13).

Pearson’s correlation. Retrieved from <https://www.statstutor.ac.uk/resources/uploaded/pearsons.pdf>.

Peng, S. (2023). Digital Economy and National Security: Contextualizing Cybersecurity-Related Exceptions. *American Journal of International Law*, 117, 122–127. <https://doi.org/10.1017/aju.2023.18>.

Petrová, K. (2022). The Impact of Digital Technologies on Neoclassical Labour Market. *Danube*, 13(4), 318–330. <https://doi.org/10.2478/danb-2022-0020>.

Pizhuk O. (2020). Cybersecurity as an acceleration factor of the digital transformation of Ukraine’s economy. *International Scientific Journal “Internauka”*. Series: “Economic Sciences”, №10, <https://doi.org/10.25313/2520-2294-2020-10>.

Revak, I. O., Gren, R. T. (2021). Peculiarities of the formation of secure cyberspace in the digital economy. *Innovative economy*, 3–4, 164–169. <https://doi.org/10.37332/2309-1533.2021.3-4.23>.

Shpak, N., Doroshkevych, K., Shpak, Y., Salata, I., Sharko, M. (2021). Strategy and tactics of international digitalization and intellectualization of economic relations. CEUR Workshop Proceedings, 2870, 1477–1487. <https://ceur-ws.org/Vol-2870/paper109.pdf>.

Teoh, C. S., Mahmood, A. K. (2017). National cyber security strategies for digital economy. *Journal of Theoretical and Applied Information Technology*, 95(23), 6510–6522.

Verma, A., Surendra, R., Reddy, B. S., Chawla P. and Soni, K. (2021). Cyber Security in Digital Sector. 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, 703–710, <https://doi.org/10.1109/ICAIS50930.2021.9395933>.

Vysochan, O., Hyk, V., Mykytyuk, N., Vysochan, O. (2023). Taxonomy of Financial Reporting in the Context of Digitalization of the Economy: Domestic and International Analysis Scientific Research. *Studia Universitatis “Vasile Goldis” Arad – Economics Series*, 33(2), 49–70. <https://doi.org/10.2478/sues-2023-0008>.

Vysochan, O., Hyk, V., Vysochan, O. (2021). Institutional theory of accounting as a tool of social ideology. *Cogito – Multidisciplinary research journal*, XIII(4), 198–208.

Vysochan, O., Vysochan, O., Chubai, V., Hyk, V., (2022). Segmentation of charitable organizations in Ukraine using clustering technology. *Quality – Access to Success*, 23(187), 102–108. <https://doi.org/10.47750/QAS/23.187.12>.

Yerina, A., Honchar, I., Zaiets, S. (2021). Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society. *Science and Innovation*, 17(3), 3–13. <https://doi.org/10.15407/scine17.03.003>.