Brunela Kullolli
Lecturer, Full Doctor at the Faculty of Political and Legal Sciences in the Aleksander Moisiu University of Durres
brunelakullolli45@gmail.com
Aibek Adanbaev
Senior Lecturer at the Department of Industrial Engineering in the Kyrgyz-Turkish Manas University
Karlis Ketners
Partnership Professor, PhD at the Faculty of Bioeconomy Development in the Vytautas Magnus University Agriculture Academy
Raimundas Jurka
Professor, PhD at the Institute of Criminal Law and Procedure in the Mykolas Romeris University
Peter Kusznieruk
Rector, Full Doctor of the Warsaw Medical Academy

Strategic approaches to ensuring information security in the context of digitalisation of economic processes

Abstract

The purpose of this study was to identify the relationship between digital security and economic sustainability in the context of digital governance transformation on the example of Albania, Lithuania, Estonia, Croatia, and the Czech Republic. The methodological framework included structural-functional analysis, processing of statistical indicators, and econometric modelling of the dependencies between the level of digital security and indicators of economic activity. Special attention was paid to the analysis of modern cybersecurity regulations adopted in 2024-2025, with a focus on sectoral regulation and the powers of national authorities. The study found that countries with greater values of the digital maturity index (up to 74.3 in Estonia) and human capital (up to 0.79), as well as with a prominent level of employee coverage by corporate cyber awareness programmes (up to 81% in the same country), demonstrated lower productivity losses due to cyber incidents, greater resilience to solvency risks (up to 0.33 in the Czech Republic), and a greater share of e-commerce in the gross domestic pro-

duct (GDP) (up to 9.8% in the Czech Republic). The active implementation of digital security tools was found to be accompanied by a decrease in the negative impact of incidents on the activities of enterprises, although in some cases (e.g., in Estonia) high losses were maintained with a small number of violations. The study determined that the introduction of cloud services and multi-level authentication is critical to increasing the adaptability of economic systems to digital challenges and reducing the overall level of vulnerability of enterprises. The summary results of the study highlighted the need to integrate technical solutions, digital education, institutional protocols, and corporate cyber hygiene culture into a single, coherent digital security strategy that factors in the specifics of national digitalisation models. The findings of this study can be used by public authorities, small and medium-sized businesses, analytical institutions, and developers of digital strategies to optimise information security management mechanisms.

KEYWORDS: Human Capital, E-Commerce, Cyber Threats, Response Coordination, Critical Infrastructure, Risk Management.

1. Introduction

The conditions of digital transformation of economic systems have led to an increase in the dependence of business entities on information and communication technologies, which actualised information security threats at the level of both enterprises and states. The increase in the intensity of cyber threats is accompanied by a more complex structure, which requires a systematic approach to risk management in the digital environment. The growing share of e-commerce in the gross domestic product (GDP), the expanding use of cloud services, Security Information and Event Management and Endpoint Detection and Response solutions, and increasing regulatory pressure require the development of an effective digital security model adapted to the specifics of national economies. The research covers the low level of digital skills among employees, fragmentation of corporate cyber awareness programmes, limited integration of technical

solutions, and insufficient inter-institutional coordination, which hinders effective response to cyber threats.

The complexity of these challenges creates the need to analyse the interrelationships between digital indicators of economic activity, institutional preparedness for cyber risks, and human potential as an element of resilience to information threats. Small and medium-sized enterprises operating in a resource-poor environment are the most susceptible to the negative effects of cyber incidents, which makes it necessary to analyse them in detail. In this context, it is essential not only to determine the level of digital maturity and implemented technologies, but also to assess the effectiveness of digital security policies in the context of Albania, Lithuania, Estonia, Croatia, and the Czech Republic, which are at different stages of digital development.

Pashaj et al.[1] found that Albania's critical information infrastructure is highly vulnerable to systemic cyber threats due to the fragmented legal framework and insufficient coordination between government agencies. The researchers found a low level of implementation of technical security protocols, which increases the risk in the context of digital transformation. Tiri and Aliaj[2] confirmed this trend, emphasising the insufficient effectiveness of the national regulator in the field of information security, despite the implementation of certain EU directives. The analysis found that the level of regulatory readiness in Albania is still below the European average, which hinders the development of the digital economy.

According to Çeko[3], the educational environment in Albania lacks a systematic approach to the training of cybersecurity specialists, which affects the overall level of digital literacy. Mockaitė[4] found that Lithuania actively employs strategic communication strategies as a tool to counter information threats, which

1 K. PASHAJ, E. GJIKA and L. BASHA, *The importance of critical information infrastructure protection – Case of Albania*, in *Journal of Natural Sciences*, 2024, 35, pp. 278–293.

2 E. TIRI and E. ALIAJ, *Cyber-security regulation in Albania*, in *Perspectives of Law and Public Administration*, 2023, 12(2), pp. 275–282.

3 E. CEKO, *Cyber security issues in Albanian higher education institutions curricula*, in *CRJ*, 2021, 1, pp. 56–65.

4 G. MOCKAITĖ, *Military and political strategic communication…*, 2024, Kaunas: Vytautas Magnus University.

allows increasing institutional resilience. Štitilis et al.[5] empirically proved the existence of a comprehensive system of hybrid cyber threats in Lithuania, which combines technical, political, and social components of influence.

Bukauskas et al.[6] identified the key competencies necessary to ensure cybersecurity in a small digital market, while emphasising the need to integrate the standards of the European e-Competence Framework. Ghelani[7] provided a global overview of the types of cyber threats and indicates that the increasing complexity of attacks requires constant updating of security protocols at the enterprise level. Olaniyi et al.[8] developed the CyberFusion model, which combines the ISO/IEC 27001 standard, mobile forensics, and risk management into a single digital security architecture, which reduces incidents in the business environment.

Yee and Zolkipli[9] empirically confirmed that maintaining the principles of confidentiality, integrity, and availability (CIA-triad) is a critical factor in preventing the compromise of digital systems. Bondarenko et al.[10] found that the effectiveness of legal mechanisms for information security in the context of digitalisation depends on the consistency between technical standards and legislative norms, as shown by the example of the European Union.

Kalinin et al.[11] created a methodology for assessing economic security in digital investment processes, which considers the risks of digital instability and allo-

5 D. STITILIS, M. LAURINAITIS and M. WARREN, *Hybrid cyber threats: Lithuanian context*, in *Journal of Information Warfare*, 2024, 23(1).

6 L. BUKAUSKAS, A. BRILINGAITĖ, A. JUOZAPAVIČIUS, D. LEPAITĖ, K. IKAMAS and R. ANDRIJAUSKAITĖ, *Remapping cybersecurity competences in a small nation state*, in *Heliyon*, 2023, 9(1), p. e12808.

7 D. GHELANI, *Cyber security, cyber threats, implications and future perspectives: A review*, 2022, 1, pp. 1-8.

8 O.O. OLANIYI, O.O. OMOGOROYE, F.G. OLANIYI, A.I. ALAO and T.O. OLADOYINBO, *CyberFusion protocols…*, in *Journal of Engineering Research and Reports*, 2024, 26(6), pp. 31–49.

9 C.K. YEE and M.F. ZOLKIPLI, *Review on confidentiality, integrity and availability in information security*, in *Journal of ICT in Education*, 2021, 8(2), pp. 34–42.

10 S. BONDARENKO, O. MAKEIEVA, O. USACHENKO, V. VEKLYCH, T. ARIFKHODZHAIEVA and S. LERNYK, *The legal mechanisms for information security in the context of digitalization*, in *Journal of Information Technology Management*, 2022, 14, pp. 25–58.

11 O. KALININ, V. GONCHAR, O. ZAKHARCHENK, O. DARUSHYN, M. MALTSEV and P. DATSIUK, *A comprehensive methodology for evaluating economic security in the digitalization of investment processes*, in *Revista de Gestão Social e Ambiental*, 2024, 18(5), p. e05441.

ws formalising the impact of cyber threats on investment projects. Kraus et al.[12] determined that the digitalisation of business processes within the Industry 4.0 paradigm creates new growth vectors, but at the same time generates risks associated with the information vulnerability of industrial platforms.

Despite the prominent level of theoretical and empirical development of certain aspects of digital security, most studies do not include a cross-country comparative analysis of the relationship between digital infrastructure, human capital, and economic vulnerability of enterprises. There are no integrated approaches to assessing the impact of corporate cyber awareness programmes on economic losses and productivity risks. The issue of optimising digital security in the context of the specifics of small economies, such as Albania, Croatia, Czech Republic, Estonia, Lithuania, and Estonia, is not sufficiently studied, considering complex institutional and technological changes.

The purpose of this study was to establish the relationship between the parameters of digital security and the economic efficiency of digital transformation on the example of Albania, Lithuania, Estonia, Croatia, and the Czech Republic – five European countries with different models of digital governance. To fulfil this purpose, the following research objectives were formulated: to characterise the institutional features of digital risk management and the structure of financial losses due to cyber incidents; to determine the degree of prevalence of information security technologies among enterprises and the level of digital maturity of the economy; to analyse indicators of human capital and coverage of corporate cyber awareness programmes; to identify statistical correlations between digital security and economic parameters, including productivity, the share of e-commerce in GDP, and solvency of business entities.

2. Materials and methods

The study employed the methodology of quantitative comparative analysis with elements of econometric evaluation and structural-functional approach. The type of research was defined as analytical, with an emphasis on cross-country comparison of statistical and regulatory indicators. The timeframe covered the

12 N. KRAUS, K. KRAUS and O. MANZHURA, *Digitalization of business processes… Industry 4.0*, in *WSEAS Transactions on Business and Economics*, 2021, 18, pp. 569–580.

period from January 2024 to May 2025, which corresponds to the current stage of implementation of digital strategies and updated information security policies in the European Union and candidate countries. The study was focused on identifying the relationships between the level of digital readiness, human capital development, and economic resilience in the face of cyber threats.

To form the empirical basis, official sources of the European Commission (n.d.) were used, specifically, the Digital Economy and Society Index database, statistical reports of the European Statistical Agency Eurostat (n.d.). The sample included Albania, Lithuania, Estonia, Croatia, and the Czech Republic as examples of countries with different depths of digital transformation, contrasting institutional models of cyber defence, and various levels of implementation of corporate and government digital literacy programmes. The choice was based on the need for representative coverage of European Union countries with distinct starting points and dynamics of digital development. To ensure the legal validity of the comparative analysis, the provisions of national cybersecurity laws adopted in 2024-2025 in Albania (Monitoring Report of the National Cyber Security Strategy 2020-2025 of Albania)[13], Lithuania (Law of the Republic of Lithuania No. XII-1428 "On Cyber Security")[14], Estonia (Cybersecurity Strategy 2024-2030 "Cyber-Conscious Estonia")[15], Croatia (Law of the Republic of Croatia No. 14/2024-254 "On Cyber Security")[16], and the Czech Republic (Law of the Czech Republic No. 181/2014 "On Cyber Security")[17] were considered. These documents outline the powers of the relevant cybersecurity authorities, define the areas of digital security regulation, and confirm the implementation of a sectoral approach to digital risk management. Additionally, for Albania, the indica-

13 *Monitoring Report of the National Cyber Security Strategy 2020–2025 of Albania*, 2024, at <https://aksk.gov.al/wp-content/uploads/2024/10/MONITORING-REPORT-.pdf>

14 *Law of the Republic of Lithuania No. XII-1428 "On Cyber Security"*, 2014, at <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee>

15 *Cybersecurity Strategy 2024–2030 "Cyber-Conscious Estonia"*, 2024, at <https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf>

16 *Law of the Republic of Croatia No. 14/2024-254 "On Cyber Security"*, 2024, at <https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html>

17 *Law of the Czech Republic No. 181/2014 "On Cyber Security"*, 2014, at <https://www.e-sbirka.cz/sb/2014/181?zalozka=text>

tors presented in the reports of the European Commission[18] were analysed, including the number of cyber incidents in SMEs, the level of basic technical protection, the coverage of employees with educational programmes, and the compliance of national legislation with the requirements of Directive of the European Parliament and of the Council No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)"[19]. In the case of Lithuania, materials from the Information Society Development Committee of Lithuania[20] were used. For Estonia, the reports of the Ministry of Economic Affairs and Communications of Estonia[21] were used. As for Croatia, information from the Croatian National Bank Cybersecurity Centre[22] and Digital Croatia Strategy 2032[23] was used. Data from the Czech Republic were obtained from the National Cyber and Information Security Agency of the Czech Republic[24].

The methodological part of the study was based on a combination of quantitative analysis of statistical indicators and the logic of comparative assessment of digital infrastructure and security policies. The content analysis of strategic documents and regulatory frameworks of the sample countries was applied, followed by coding of variables using formalised scales. The existence of a sectoral approach to information security management was determined in a binary for-

18 EUROPEAN COMMISSION, *Albania 2024 Report*, 2024, at <https://enlargement.ec.europa.eu/document/download/a8eec3f9-b2ec-4cb1-8748-9058854dbc68_en?filename=Albania%20Report%202024.pdf

19 *Directive of the European Parliament and of the Council No. 2022/2555*…, 2022, at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555>

20 INFORMATION SOCIETY DEVELOPMENT COMMITTEE OF LITHUANIA, *Information Society Progress Indicators*, 2024, at <https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/governance-lithuania>

21 MINISTRY OF ECONOMIC AFFAIRS AND COMMUNICATIONS OF ESTONIA, *Cyber Security in Estonia*, 2023, at <https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf>

22 CROATIAN NATIONAL BANK CYBERSECURITY CENTRE, *NIS2 Transposition into Croatian National Legislation*, 2024, at <https://www.advantageaustria.org/hr/NIS2_Transposition_in_Croatia_ZG.pdf>

23 *Digital Croatia Strategy 2032*, 2022, at <https://commission.europa.eu/projects/adoption-digital-croatia-strategy-2032_el>

24 NATIONAL CYBER AND INFORMATION SECURITY AGENCY OF THE CZECH REPUBLIC, *Publications & Reports*, n.d., at <https://nukib.gov.cz/en/infoservis-en/publications-reports/>

mat: a value of 1 meant the existence of an institutionalised approach at the level of relevant ministries or agencies, while 0 meant its absence. For indicators such as the Human Capital Index and the e-Government Development Index[25], a scale from 0 to 1 was used, where values closer to 1 indicated a greater level of human capital or digital infrastructure development, respectively.

The technological equipment of enterprises was analysed by summarising national indicators for the implementation of key cybersecurity solutions, including threat detection systems, endpoint protection solutions, and multi-level authentication. For all variables of this type, a relative scale with a 100% threshold was used – the share of enterprises declaring the implementation of the relevant technology was interpreted as a percentage. An analogous approach was applied to the Digital Skills Indicator, which was defined as the percentage of the population demonstrating basic or above basic digital skills according to the Eurostat classification. For the indicator of the digital maturity of the economy and the share of e-commerce in the structure of GDP, a scale of 0-100% was used to ensure consistency with Digital Economy and Society Index statistical reports[26].

A multi-level gradation was used to estimate economic losses from cyber incidents by category of enterprise (small, medium, large). The "small" category included enterprises with up to 50 employees and a turnover of up to EUR 10 million; "medium" – up to 250 employees and up to EUR 50 million, respectively; "large" – above these thresholds. For each category, the average losses incurred in 2024 were recorded, as well as the number of documented cyber incidents per enterprise. To model the relationships between digital risks and economic performance, the Ordinary Least Squares method was used for continuous variables (productivity, turnover) and logistic regression for probabilistic variables (loss of solvency, business interruption). The values of the regressors were normalised within the interval from -1 to +1, which allowed quantifying the strength and vector of the impact of the respective digital factor on the economic result. All models were based on cross-country comparisons using unified scales of variables: relative losses, digital competence indices, digital coverage, incident rate, etc.

25 WORLD BANK, *E-Government Development Index*, n.d., at <https://data360.worldbank.org/en/dataset/UN_EGDI>

26 EUROPEAN COMMISSION, *Digital Economy and Society Index*, n.d., at <https://digital-strategy.ec.europa.eu/en/policies/desi>

The e-commerce indicator was calculated as the share of the value of online sales in the structure of the GDP of the respective country. It was based on annual Eurostat[27] data on the volume of digital transactions in the corporate sector. The Digital Economy and Society Index was integrated with the e-commerce indicator through the inclusion of the index of digital integration of business as one of the key components of overall digital maturity. This helped to investigate the extent to which the level of digital transformation of enterprises is related to the dynamics of e-commerce development and financial sustainability of business entities.

The results were interpreted considering the correlation structure of dependencies between individual indicators. Changes in the aggregate digital security indicators over time, the ratio of technological readiness and factual resilience to cyber threats, and the relationship between the population's digital skills and the level of losses from incidents were considered. The principle of comparison between countries with high and low values of key indicators was applied, which helped to identify generalised models of economic response to digital challenges. To verify the significance of the results, the study employed confidence interval criteria with a statistical error level not exceeding 5%.

3. Results

3.1. Regulatory and institutional framework for ensuring information security in the context of digital transformation of the economy

In building a national information security system, the key role is played by regulations that establish requirements for digital protection at all levels of the economy. In the context of harmonisation with the EU legislation, the countries of Eastern and Southern Europe and the Baltic States are reviewing their strategic and legal approaches to cyber resilience, adapting them to the provisions of Directive of the European Parliament and of the Council No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)" and other sectoral docu-

27 EUROSTAT, *Statistical data on digital economy and society*, n.d., at <https://ec.europa.eu/eurostat>

ments. Considering these transformations, it is advisable to summarise the main characteristics of the latest cybersecurity regulations adopted in 2024-2025 in Albania, Lithuania, Estonia, Croatia, and the Czech Republic (Table 1).

Table 1. Key parameters of cybersecurity legislation (2024-2025)

Country	Title of the legislative act	Competent authority	Areas of coverage	Availability of a sectoral approach
Albania	Law No. 25/2024 on Cybersecurity (2024)	National Directorate for e-Governance and Cybersecurity	Critical infrastructure, telecoms, civil service	Yes
Lithuania	Law on Cybersecurity (2018, revision 2024)	National Cyber Security Centre under the Ministry of Defence	Digital services, defence, finance	Yes
Estonia	Law on Cybersecurity within the framework of the Strategy 2024-2030 (2024)	Information System Authority	Public services, infrastructure, digital governance	Yes
Croatia	Law on Cybersecurity (2024)	National Cyber Defence Centre at the Ministry of the Interior	Service operators, public institutions, energy sector	Yes
Czech Republic	Law on Cybersecurity (2025)	National Agency for Cyber and Information Security	Business, critical suppliers, Industry 4.0	Yes

[Note: the clarification of the names of some bodies is adapted to the official abbreviations in regulatory documents]

[Source: developed by the authors based on data from Monitoring Report of the National Cyber Security Strategy 2020-2025 of Albania, Law of the Republic of Lithuania No. XII-1428 "On Cyber Security", Cybersecurity Strategy 2024-2030 "Cyber-Conscious Estonia", Law of the Republic of Croatia No. 14/2024-254 "On Cyber Security", and the Law of the Czech Republic No. 181/2014 "On Cyber Security"]

The comparative analysis revealed a significant degree of unification in the formal cybersecurity frameworks implemented in the countries under study. All

five countries adapted their national legislation to the requirements of NIS2, ensuring the establishment of a competent authority, expanding the scope of coverage, and introducing a sectoral approach to risk management. A gradual detailing of the laws towards the separation of the public and private sectors is observed, which is particularly pronounced in the Czech Republic and Lithuania. Although all countries formally adopt a sectoral approach, the scope of regulatory instruments varies significantly, indicating differences in practical implementation. The structure of the competent authorities also demonstrates varying degrees of centralisation: from integrated information agencies (Estonia) to specialised bodies within ministries (Croatia, Lithuania).

In building an effective digital security system, one of the key conditions is the existence of an institutionally capable specialised body responsible for implementing cybersecurity policy[28]. In Central and Eastern Europe, such structures operate with varying degrees of centralisation, which affects both the quality of oversight and the ability to respond quickly to incidents. A significant sign of institutional effectiveness is also the existence of formalised mechanisms for interagency cooperation, especially in the context of the cross-influence of digital risks across multiple sectors of the economy. Table 2 presents a comparison of the institutional architecture of cybersecurity bodies in Albania, Croatia, Czech Republic, Estonia, Lithuania, and Estonia.

Table 2. Institutional structure of cybersecurity authorities in selected countries (2024-2025)

Country	Specialised body	Centralisation level	Control and monitoring functions	Interagency cooperation
Albania	National Directorate for e-Governance and Cybersecurity	High (single coordinating body)	Oversight, audit, incident investigation	Through the interagency cybersecurity council
Lithuania	National Cyber Security Centre under the Ministry of	Medium (separation from the MoD)	Inspections, compliance checks, certification	Joint platforms with defence and digital ministries

28 B. ABDYGALYM, M. SAMBETBAYEVA, A. YERIMBETOVA, A. NEKESSOVA, N. TASBOLATULY, N. SMAILOV and A. NAZYMKHAN, *NLP models for military terminology analysis and detection of information operations on social media*, in *Computers*, 2025, 14(11), p. 485.

	Defence			
Estonia	Information System Authority	High (centralised through Information System Authority)	Real-time monitoring, response, audits	Integrated communication protocols with all sectors
Croatia	National Cyber Defence Centre at the Ministry of Interior	Medium (shared between the MoI and sectoral agencies)	Monitoring, technical expertise, Computer Emergency Response Team coordination	Through an interagency working group under the government
Czech Republic	National Agency for Cyber and Information Security	High (central regulator)	Conformity assessment, supervision, response coordination	Formalised coordination with government and business structures

[Source: developed by the authors based on from European Commission, Eurostat, Monitoring Report of the National Cyber Security Strategy 2020-2025 of Albania, Law of the Republic of Lithuania No. XII-1428 "On Cyber Security", Cybersecurity Strategy 2024-2030 "Cyber-Conscious Estonia", Law of the Republic of Croatia No. 14/2024-254 "On Cyber Security", and the Law of the Czech Republic No. 181/2014 "On Cyber Security"]

A comparative analysis of Table 2 revealed that all five countries have a stable specialised cybersecurity body that meets the basic requirements of NIS2. However, the level of centralisation of these structures varies considerably: in the Czech Republic, Estonia, and Albania, there is a clear centralised management, while in Lithuania and Croatia, functions are distributed among several administrative entities. This leads to differences in day-to-day incident response mechanisms, institutional accountability, and the quality of oversight. The role of interagency cooperation is particularly significant in the context of multi-sectoral risks, where the degree of synchronisation between government agencies, the defence sector and private companies is crucial. The Czech Republic has a strong degree of formalisation of cooperation, while Croatia and Albania use interagency councils as the principal format of coordination.

The assessment of the regulatory potential in the field of information security should be supplemented with quantitative indicators that characterise the le-

vel of digital maturity of public administration and regulatory readiness to counter cyber threats. In this context, it is advisable to use two integrated indices: The e-Government Development Index, which measures the ability of a state to provide digital services, and the Global Cybersecurity Index, which measures the capacity of state institutions to ensure cybersecurity. The analysis of data for 2024 and the assessment of expected values for 2025 allow establishing the dynamics of regulatory strengthening and the effectiveness of national strategies (Figure 1). This approach helps not only to compare countries with each other, but also to identify patterns between institutional modernisation and the level of digital governance.

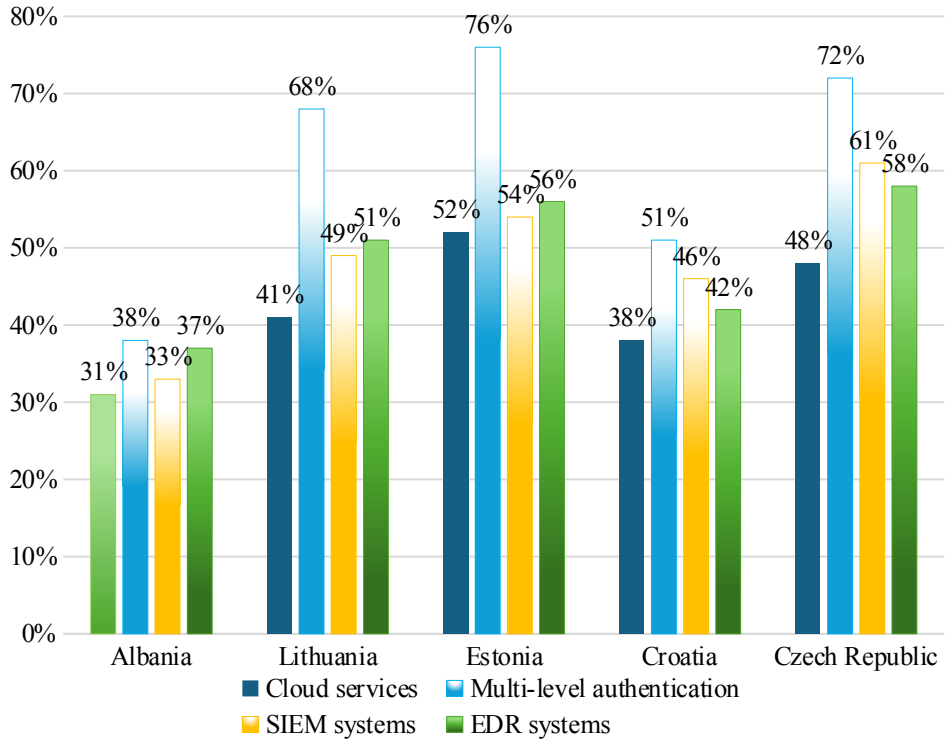

Fig. 1. Indices of digital maturity and regulatory readiness (2024-2025)

[Source: developed by the authors based on data from European Commission, Eurostat]

Analysis of Figure 1 shows an overall positive trend in both digital maturity and regulatory readiness in all five countries. Estonia maintains its leading position in both the e-Government Development Index and Global Cybersecurity Index, demonstrating the highest degree of alignment between digital gover-

nance and cyber defence. Lithuania and the Czech Republic also show consistently high scores, with little progress for 2025, which correlates with institutional centralisation and the implementation of strategic plans. Albania, albeit having the lowest values among the countries analysed, shows a significant increase, which indicates the effectiveness of the implementation of the new legislation. Croatia is at the middle level, but the dynamics of its improvement are less pronounced, which may suggest limited institutional flexibility or fragmented implementation of the digital security strategy.

3.2. Economic impact of digital threats on business: analytical assessment of risks and losses

In the context of growing digital threats, quantifying the real economic consequences that businesses suffer as a result of information security breaches is of particular significance. The experience of the five countries under study showed that small and medium-sized enterprises are still the most vulnerable to cyberattacks, due to limited access to specialised cyber defence technologies and a lack of specialised competencies. Therewith, extensive financial losses are also recorded in the large business segment, particularly in areas that are critically dependent on digital technologies, such as industrial production, logistics, and energy. Considering this, it is advisable to present a generalised empirical picture that combines data on the number of registered cyber incidents and an estimate of direct economic losses, differentiated by type of enterprise. Such detailing allows identifying differences in the structure of risks depending on the organisational and economic scale of companies. Table 3 presents the volume of recorded cybersecurity breaches and the corresponding financial losses for small, medium, and large businesses in the five countries studied in 2024.

Table 3. Number of cyber incidents and direct economic losses for businesses in 2024 (by business size)

Country	Incidents (small)	Incidents (medium)	Incidents (large)	Losses (small), EUR mn	Losses (medium), EUR mn	Losses (major), EUR mn
Albania	157	62	21	4.3	2.6	1.1
Lithuania	121	78	32	5.1	4.2	2.3
Estonia	108	84	29	6.7	4.9	3.2
Croatia	94	66	27	3.9	2.8	1.7

Czech Republic	87	71	36	4.8	3.5	3

[Note: the number of incidents is recorded according to the criteria of national cyber monitoring systems; losses reflect only direct losses (including operational, technical, and legal costs) without considering loss of reputation or indirect effects]

[Sources: developed by the authors based on data from Eurostat]

The analysis of Table 3 shows a high concentration of cyber incidents in the small business segment in all five countries, which is accompanied by substantial financial losses. The highest burden in terms of the number of incidents was observed in Albania (157 cases), but Estonia suffered the largest economic losses among small businesses (EUR 6.7 mn), which indicates the depth of the impact of cyber incidents on the financial stability of digitally integrated businesses. In the medium-sized segment, the largest losses were also recorded in Estonia (EUR 4.9 million) and Lithuania (EUR 4.2 mn), which correlates with a prominent degree of digital integration but also increased risk. In the large enterprise sector, the Czech Republic demonstrates the greatest number of incidents (36) with corresponding losses of EUR 3 mn, which is explained by the diverse industrial structure of the economy. The findings confirmed the need for a differentiated approach to risk management depending on the size of the enterprise and the level of digital maturity.

In the study of the effects of digital threats on business activities, the key role is played by econometric assessment, which enables quantitative verification of the relationship between the frequency of cyber incidents and financial and economic indicators. Particular attention was paid to three variables: labour productivity, turnover, and the ability of enterprises to maintain solvency after an incident. Modelling was performed using the Ordinary Least Squares method and logistic regression, which helped to obtain estimates of both continuous and probabilistic changes. Table 4 summarises the results of the models for Albania, Croatia, Estonia, Lithuania, and the Czech Republic.

Table 4. Results of econometric models on digital risks in business (2024)

Country	Ordinary Least Squares coefficient	Ordinary Least Squares coefficient	Probability of losing solvency (logit model)	Probability of business interruption >24

	(productivity)	(turnover)		hours (logit model)
Albania	-0.38	-0.34	0.41	0.28
Lithuania	-0.26	-0.22	0.36	0.24
Estonia	-0.31	-0.25	0.32	0.22
Croatia	-0.29	-0.24	0.39	0.27
Czech Republic	-0.27	-0.21	0.33	0.26

[Note: logit model – logistic regression to estimate the probability of an event occurring; "productivity" – the ratio of gross value added to the number of employees; "turnover" – total revenue from sales of goods and services for a calendar year. The values of the Ordinary Least Squares coefficients reflect the change in the dependent variable with each added incident; probabilities in logit models are estimated values based on the regression function]

[Source: developed by the authors based on data from European Commission, Directive of the European Parliament and of the Council No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)", Information Society Development Committee of Lithuania, Ministry of Economic Affairs and Communications of Estonia, Croatian National Bank Cybersecurity Centre, Digital Croatia Strategy 2032, National Cyber and Information Security Agency of the Czech Republic (n.d.), World Bank]

The results of Table 4 show a significant negative impact of digital incidents on key financial and economic indicators of enterprises in all five countries. The greatest level of sensitivity to productivity decline is observed in Albania (-0.38), which indicates a significant drop in business performance in the face of cyber risks. Estonia demonstrates a less negative impact in terms of turnover (-0.25) but is more effective in deterring business interruption (>24 hours), indicating a better balance between digital vulnerability and reactive capacity. The Czech Republic has the lowest probability of losing solvency among the countries analysed (0.33), which may be due explained by the higher penetration of certified cyber defence systems. Lithuania and Croatia occupy intermediate positions but show a sharper reaction in cases of logistical and reputational disruptions. The consolidated data set confirmed the need not only to respond to incidents, but also to implement a preventive risk management model as an economic function of digital threat management.

3.3. Technological infrastructure and innovative solutions as factors of resilience to information threats

The intensity of the implementation of technological solutions in the field of information security is a significant criterion for the resilience of digital infrastructure. Businesses operating in a highly digitalised environment are forced to adapt their risk management systems to meet the growing range of cyber threats. The use of cloud services, multi-level authentication, security event analysis systems, and endpoint security tools ensures rapid response, reduces the probability of compromising digital assets, and increases trust in digital business platforms.

To compare the level of technological readiness of business entities in Albania, the Czech Republic, Estonia, Lithuania, Croatia, and the Czech Republic, the share of enterprises that used key information security tools as of 2024 was summarised (Figure 2). The data covers four technology categories that are recognised as critical in digital transformation policies: cloud services, multi-level authentication, Security Information and Event Management and Endpoint Detection and Response systems.

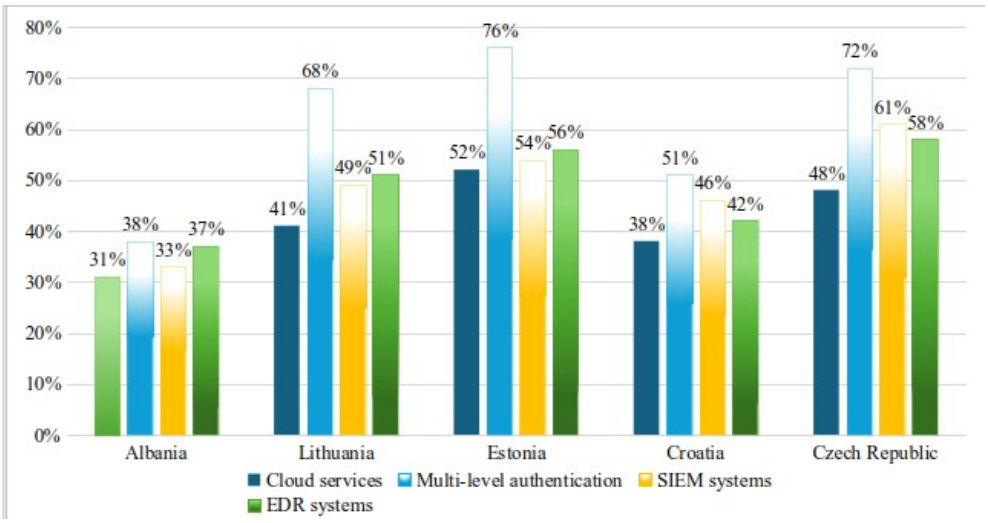

Fig. 2. Share of enterprises using basic information security technologies in 2024 (% of the total number of companies)

[Source: developed by the authors based on data from European Commission, Directive of the European Parliament and of the Council No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)", Information Society Development Committee of Lithuania, Ministry of Economic Affairs and Communications of Estonia, Croatian National Bank Cybersecurity Centre, Digital Croatia Strategy 2032, National Cyber and Information Security Agency of the Czech Republic, World Bank]

The analysis of Figure 2 shows significant differences in the degree of implementation of information security technologies between the countries under study. Estonia and the Czech Republic demonstrate the greatest values, where more than half of enterprises use cloud services, multi-level authentication, Security Information and Event Management, and Endpoint Detection and Response. In Lithuania, the level of technological integration is somewhat lower, but consistently exceeds the EU average in the SME (small and medium-sized enterprises) segment. Croatia and especially Albania are falling behind in all respects, indicating a need for stronger institutional incentives for digital modernisation. Overall, Figure 2 illustrates the direct correlation between the development of digital security and the overall digital maturity of an economy.

The level of digital maturity of the economy and the volume of e-commerce in the structure of GDP form key indicators of a country's ability to adapt to the challenges of the digital environment (Table 5). These parameters reflect both the technical infrastructure and the degree to which digital solutions are integrated into everyday business practices. Of particular significance is the correlation between the Digital Economy and Society Index and the share of e-commerce, as it allows assessing the effectiveness of digital policies in terms of economic performance. This approach was employed to conduct a comparative analysis of five countries to identify patterns of digital growth.

Table 5. Digital maturity and share of e-commerce in GDP in 2024

Country	Digital Economy and Society Index	Share of e-commerce in GDP (%)
Albania	46.1	4.9
Lithuania	59.8	7.2
Estonia	74.3	8.6
Croatia	57.5	5.7
Czech Republic	69.2	9.8

[Note: e-commerce – electronic commerce estimated as a share of total GDP based on national macroeconomic statistics and digital trade reports]

[Source: developed by the authors based on data from European Commission, Directive of the European Parliament and of the Council No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)", Information Society Development Committee of Lithuania, Ministry of Economic Affairs and Communications of Estonia, Croatian National Bank Cybersecurity Centre, Digital Croatia Strategy 2032, National Cyber and Information Security Agency of the Czech Republic, World Bank]

The analysis of Table 5 confirms the existence of a stable positive correlation between the level of digital maturity and economic activity in the field of e-commerce. The Czech Republic (Digital Economy and Society Index – 69.2, e-commerce share – 9.8 %) and Estonia (Digital Economy and Society Index – 74.3, e-commerce – 8.6 %) demonstrate the greatest values for both indicators, which indicates the successful integration of digital solutions into business operations and system support for e-commerce. Lithuania, with a Digital Economy and Society Index of 59.8 and an e-commerce share of 7.2%, occupies an intermediate position with a fairly strong level of digital development and a steady increase in online sales. At the same time, Croatia (Digital Economy and Society Index – 57.5; e-commerce – 5.7%) and especially Albania (Digital Economy and Society Index – 46.1; e-commerce – 4.9%) show lower indicators, which may be the result of limited institutional support for digital entrepreneurship or fragmented implementation of technical tools. Overall, these dynamics point to the need to align technological potential with economic models of digitalisation to achieve full-scale scaling effects in the digital economy.

3.4. Human capital potential and information security culture in the context of economic digitalisation

The level of human capital development and digital skills of the population are fundamental variables that determine the ability of states to respond sustainably to information threats in the digitalised economy. Indicators that measure these aspects allow assessing both the potential of national education systems and the degree of adaptation of the workforce to the requirements of the digital market. In the context of ensuring information security, these parameters are indirect but key indicators of the overall readiness of society for cyber risks. A prominent level of digital competences directly affects the effectiveness of data protection measures in business, public administration, and everyday digital

consumption[29].

To assess the relationship between human capital development and the level of digital security, a comparative assessment of two comprehensive indicators was performed: Human Capital Index and Digital Skills Indicator in five countries of the region (Table 6). The data presented for 2024 allows not only comparing the overall level of human development but also identifying structural differences in aspects of digital training of the population. This approach is relevant for formulating recommendations for further investment in education and retraining in the field of information security.

Table 6. Human capital and digital skills indices in five countries in 2024

Country	Human Capital Index (2024)	Digital Skills Indicator (2024)
Albania	0.58	45.2
Lithuania	0.71	63.4
Estonia	0.79	72.1
Croatia	0.68	58.7
Czech Republic	0.75	66.5

[Note: Human Capital Index is a composite indicator of the World Bank that assesses the level of education, health, and expected productivity of the population; Digital Skills Indicator is a metric of the European Commission that measures the availability of basic and advanced digital competencies among working-age people]

[Source: developed by the authors based on data from European Commission, Directive of the European Parliament and of the Council No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)", Information Society Development Committee of Lithuania, Ministry of Economic Affairs and Communications of Estonia, Croatian National Bank Cybersecurity Centre, Digital Croatia Strategy 2032, National Cyber and Information Security Agency of the Czech Republic, World Bank]

Analysis of Table 6 shows a clear correlation between the level of general human capital and digital skills. The greatest values of both indicators are recorded in Estonia: 0.79 for the Human Capital Index and 72.1% for the Digital Skills Indicator, indicating an in-depth integration of digital competences into the education, healthcare, and training systems. The Czech Republic (0.75 and

29 S. KENGESBAYEVA, A. RAZAQUE, N. SMAILOV, Z. KALPEYEVA and U.R. KABIEVNA, *Optimizing resource allocation for 5G Internet-of-Things networks using machine learning techniques*, in *2025 IEEE 1st Secure and Trustworthy Cyberinfrastructure for IoT and Microelectronics, Conference Proceedings*, Institute of Electrical and Electronics Engineers, Dayton, 2025.

66.5%) and Lithuania (0.71 and 63.4%) show relatively balanced development, indicating a steady combination of institutional capacity and the adoption of digital practices. Croatia has a human capital index of 0.68 and a digital skills index of 58.7%, which may indicate regional disparities or fragmentation of educational and digital initiatives. Albania has the lowest indicators (0.58 and 45.2%, respectively), which indicates the need for comprehensive structural investments in human development, including digital literacy, as these aspects directly affect the state's ability to ensure effective cybersecurity.

The effectiveness of information security largely depends on the level of staff awareness, particularly in the context of detecting phishing attacks, malware, and other typical threats. In this regard, the role of corporate digital security literacy programmes is important. Such programmes are implemented at the level of enterprises and institutions of various sizes and demonstrate significant differences in terms of the scope of employee coverage, regularity of implementation, and the format of the activities involved. An empirical analysis of such programmes in five countries reveals the correlation between information security culture and the level of digital resilience (Table 7).

Table 7. Comparison of corporate information security awareness programmes in five countries (2024)

Country	Employee coverage (%)	Frequency of events	Types of activities
Albania	37	Annually	Online tutorials
Lithuania	68	Once every six months	Online courses, quizzes
Estonia	81	Quarterly	Phishing simulations, trainings
Croatia	59	Annually	Video tutorials, memos
Czech Republic	74	Quarterly	Trainings, phishing simulations

[Note: the table shows the typical formats of training events used in internal corporate information security awareness programmes. Phishing simulations – specially created emails that simulate phishing attacks to diagnose the level of employee training. The regularity of training events, interactivity of the material and the level of staff coverage are critical factors in the formation of an effective information security culture, which should be considered when developing strategies at the state and corporate levels]

[Source: developed by the authors based on data from European Commission, Directive of the European Parliament and of the Council No. 2022/2555 "On Measures for a High Common Level of Cybersecurity

Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)", Information Society Development Committee of Lithuania, Ministry of Economic Affairs and Communications of Estonia, Croatian National Bank Cybersecurity Centre, Digital Croatia Strategy 2032, National Cyber and Information Security Agency of the Czech Republic, World Bank]

The analysis of Table 7 reveals significant differences in the organisation of corporate cybersecurity training programmes in the five countries studied. The greatest level of employee coverage of these events was recorded in Estonia (81 %) and the Czech Republic (74 %), where the highest frequency of their conduct is also observed – quarterly. These countries use interactive training methods, such as phishing simulations, situational tests, and practical training, which ensures high staff involvement and creates an internal culture of responsibility for information security. This approach enhances the organisations' ability to respond to digital threats and reduces the probability of human error in breaching internal security protocols.

In Lithuania, corporate training initiatives are based primarily on online courses supplemented by gamification elements such as quizzes and interactive tests. This form of presentation ensures accessibility of the material and reaches a wide audience but is inferior to Estonia and the Czech Republic in terms of intensity and practical orientation of training. In Croatia and Albania, the level of employee participation in relevant programmes is significantly lower, with only 37% in Albania. The key form of training in these countries is limited to one-off briefings and standard presentations, which does not allow for sustainable learning of skills and the formation of behavioural models of cyber hygiene. The limited frequency and lack of an adaptive approach reduce the effectiveness of such measures, especially in the context of the dynamic growth of digital risks.

Summarising the above, there is arguably a direct link between the intensity of corporate cyber education programmes and the effectiveness of digital security policies at the micro level. Countries with a higher proportion of employee coverage, regular training, and the use of innovative methods demonstrate greater adaptability to digital challenges and better economic resilience in the face of cyber threats. This highlights the need to institutionalise corporate training practices as one of the key elements of the national cyber strategy.

To systematise the institutional state of implementation of digital security strategies in Albania, Croatia, Czech Republic, Estonia, Lithuania, and Estonia, a comparative expert assessment of the strengths and weaknesses of national cyber defence models was conducted. The Table 8 summarises the results of the assessment by the criteria of strategic comprehensiveness, best practices, and key challenges in the implementation of digital policies. It serves as a basis for proceeding to a more in-depth analytical summary of the reasons for the vulnerability of certain elements of the cybersecurity system and the effectiveness of the approaches used to reduce digital risks.

Table 8. Comparative assessment of the strategic level, practices and identified gaps in cybersecurity (2024-2025)

Country	Level of strategic complexity	Most characteristic strengths	Key weaknesses/implementation challenges
Estonia	Most comprehensive strategy (Strategy 2024-2030, Information System Authority integration)	High digital integration, clear role of the regulator, coverage of digital education	High losses even with developed infrastructure; sensitivity of complex systems
Czech Republic	High	Stable regulatory framework, clear governance (National Agency for Cyber and Information Security), sector specificity	Insufficient coverage of SMEs by cyber education programmes; gap between sectors
Lithuania	Medium	Coordination at the level of the Ministry of Defence, digital services	Moderate coverage of monitoring technologies; uneven regional implementation
Croatia	Medium	National centre under the Ministry of Interior, focus on public sector	No long-term strategy; fragmented policies
Albania	Lowest coherence	Updated law in 2024, establishment of a national	High number of incidents, low level of

		body	digital skills, limited institutional resources

[Source: developed by the authors based on the findings and data from Monitoring Report of the National Cyber Security Strategy 2020-2025 of Albania, Law of the Republic of Lithuania No. XII-1428 "On Cyber Security", Cybersecurity Strategy 2024-2030 "Cyber-Conscious Estonia", Law of the Republic of Croatia No. 14/2024-254 "On Cyber Security", and the Law of the Czech Republic No. 181/2014 "On Cyber Security", European Commission, Directive of the European Parliament and of the Council No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)", Information Society Development Committee of Lithuania, Ministry of Economic Affairs and Communications of Estonia, Croatian National Bank Cybersecurity Centre, Digital Croatia Strategy 2032, National Cyber and Information Security Agency of the Czech Republic, World Bank]

A summary of the results of Table 8 shows significant differences between countries in the degree of development of cybersecurity systems. Estonia provides the most comprehensive model of protection, characterised by in-depth integration of digital technologies, centralised management through Information System Authority, and regular employee training programmes. However, the complexity of the digital infrastructure results in residual vulnerability to incidents. The Czech Republic demonstrates high regulatory stability and a clear functional division of responsibilities (National Agency for Cyber and Information Security) but faces insufficient support for small businesses in digital awareness. Lithuania and Croatia are implementing point institutional initiatives, particularly in multi-level authentication and monitoring, but lack strategic coordination. Albania, despite the adoption of updated legislation, continues to be the country with the lowest level of institutional readiness, which is reflected in the high number of incidents and poor digital literacy of its staff.

A critical analysis of the findings revealed a strong correlation between the level of digital maturity, the prevalence of information security technologies, and economic resilience to digital risks in the countries studied. Specifically, countries with a high human capital index (over 0.75) and a high coverage of employees with cyber awareness education programmes (over 70%), such as the Czech Republic and Estonia, experienced a reduction in productivity losses and a lower frequency of critical incidents. Meanwhile, in Croatia and Lithuania, the active implementation of multi-level authentication tools, event detection, and incident response systems, which reduced the vulnerability of small and medium-sized businesses, provided a positive trend.

The study findings also point to a close link between the regulatory and institutional framework and the economic capacity of states to counter information threats. It was found that countries with a prominent level of harmonisation of national legislation with the provisions of the European Union Directive of the European Parliament and of the Council No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)" demonstrate a greater degree of integration of cybersecurity into general economic management. The centralised architecture of institutional responsibility for monitoring, responding to and preventing incidents is particularly effective, as seen in the examples of Estonia and the Czech Republic. At the same time, in countries with fragmented structures and insufficient resources (such as Albania), such functions are implemented to a limited extent.

An in-depth analysis of the economic impact of cyber incidents showed the existence of correlations between the frequency of digital attacks and key indicators of economic activity of enterprises. The econometric models built confirmed a statistically significant relationship between the level of digital security and indicators of productivity, turnover, and solvency. Countries with greater values of the e-Government Development Index and the Global Cybersecurity Index suffered lower economic losses, which indicates the effectiveness of institutional and technical cooperation as a foundation for economic resilience.

Apart from regulatory and institutional factors, the level of technical infrastructure and the quality of human capital play a special role. The study found that countries with active implementation of cloud technologies, Security Information and Event Management, and Endpoint Detection and Response systems, as well as large-scale digital education programmes, demonstrate higher e-commerce and the share of digital products in GDP. At the same time, the imbalance in the development of digital skills of the population and the limited coverage of educational initiatives continue to be the vulnerabilities that require strategic intervention by the public administration and the private sector.

4. Discussion

The findings obtained showed that there are significant differences in approaches to digital security across countries, which are conditioned by differences in the level of development of the regulatory and institutional environment, digital infrastructure, and human capital. The identified imbalances in the effectiveness of cybersecurity policies demonstrate the complex nature of the relationship between technological readiness and economic resilience to information threats. In this context, striking a balance between technical tools, institutional support, and the development of digital competencies of personnel is of particular relevance. In countries with a prominent level of digital integration, solutions based on systems for monitoring security events and detecting and responding to threats on endpoints were more often implemented, which helped to reduce the sensitivity to incidents and optimise response times[30]. This aspect was highlighted by Saeed et al.[31], proving that strategic adaptation to digital risks is a critical condition for the continuity of business processes, especially in highly dynamic sectors. It was found that in the context of digital maturity, the effectiveness of cyber defence measures is largely determined not only by the availability of technological solutions, but also by the level of corporate readiness for risk management, including established protocols, security policies and internal communication.

The empirical analysis also found that the degree of regulatory readiness of countries determines the scenarios for the use of state mechanisms in the field of digital security. Differences in legislative approaches substantially affect the adaptability of infrastructure to external threats, which was confirmed by Kulugh et al.[32], who presented a model for assessing the cyber resilience maturity of critical national information systems. According to the analysis, countries with fragmented legislative frameworks demonstrated lower efficiency of security measures, which is fully consistent with the barriers identified within the countries under

30 O. JOSEPH and I. AVIV, *Quantum-secure coherent optical networking for advanced infrastructures in Industry 4.0*, in *Information*, 2025, 16(7), p. 609.

31 S. SAEED, S.A. ALTAMIMI, N.A. ALKAYYAL, E. ALSHEHRI and D.A. ALABBAD, *Digital transformation and cybersecurity challenges…*, in *Sensors*, 2023, 23(15), p. 6666.

32 V.E. KULUGH, U.M. MBANASO and G. CHUKWUDEBE, *Cybersecurity resilience maturity assessment model…*, in *SN Computer Science*, 2022, 3(3), p. 217.

study.

Special attention was paid to the role of human capital in enhancing cyber resilience. Interpretation of the digital literacy index and digital skills data revealed a strong link between the level of investment in digital skills development and a reduction in the frequency of large-scale cyber incidents[33,34]. The findings were consistent with the study by Garcia-Perez et al.[35], who proved that effective staff training is a key factor in maintaining the functional stability of organisations during attacks on digital infrastructure. The findings showed that continuous professional development of employees, particularly in the form of internal trainings and certifications, formed an internal reserve of resilience to threats.

Furthermore, a direct correlation was established between the level of digital maturity of enterprises and the efficiency of e-commerce. In countries where digital integration was systemic, the share of e-commerce in the structure of GDP exceeded the European average, indicating a positive impact of digital practices on economic activity[36,37]. This position was confirmed by Robertson et al.[38], who noted that organisations with a strong level of digital maturity demonstrated greater adaptability to crisis challenges, particularly in the context of the COVID-19 pandemic. Thus, the strategic digitalisation of business processes is not only a means of increasing competitiveness, but also a tool for the long-term stabilisation of economic systems.

---

33 N. SMAILOV, R. KADYROVA, K. ABDULINA, F. URALOVA, N. KUBANOVA and A. SABIBOLDA, *Application of facial recognition technologies for enhancing control in information security systems*, in *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska*, 2025, 15(3), pp. 55–58.

34 V. SALMANOV and N. MAHMUDOV, *Existence of the solution of a discrete optimal control problem for linear concentrated systems with lions special quality test*, in *2012 4th International Conference Problems of Cybernetics and Informatics, Proceedings*, Baku, 2012, pp. 1–4.

35 A. GARCIA-PEREZ, J.G. CEGARRA-NAVARRO, M.P. SALLOS, E. MARTINEZ-CARO and A. CHINNASWAMY, *Resilience in healthcare systems: Cyber security and digital transformation*, in *Technovation*, 2023, 121, p. 102583.

36 N. DOLZHENKO, I. ASSILBEKOVA, Z. KONAKBAY, O. GARMASH and G. MURATBEKOVA, *Organization of transport services and transport process safety*, in *Periodica Polytechnica Transportation Engineering*, 2025, 53(3), pp. 277–291.

37 S. STEFANOV, D. GEORGIEVA and J. VASILEV, *Issues in the disclosure of financial information by multinational enterprises*, in *TEM Journal*, 2022, 11(1), pp. 5–12.

38 J. ROBERTSON, E. BOTHA, B. WALKER, R. WORDSWORTH and M. BALZAROVA, *Fortune favours the digitally mature…*, in *International Journal of Retail & Distribution Management*, 2022, 50(8/9), pp. 1182–1204.

The study analysed the relationship between sectoral digitalisation programmes and the ability of SMEs to adapt zero-trust architecture models. The findings showed that the success of such implementation largely depended not only on technical training, but also on the level of marketing adaptability and digital competence. The generalisations presented in the systematic review by Hokmabadi et al.[39] confirmed that the combination of digital skills and marketing capabilities is a key factor in the adaptation of small businesses to new digital realities. This provision is consistent with the findings of the present study, which revealed a high dependence of the effectiveness of the implementation of digital security protocols on the multidisciplinary maturity of enterprises.

The analysis of the model of interdependence between the degree of digital transformation and the organisational structure of cyber defence systems confirmed the value of systematic management of security processes. Lampe[40] presented a conceptual model of the Circular Interaction Model, which offered a step-by-step reverse adjustment of risks based on the interaction of technical and managerial levels. The application of this approach allows achieving a prominent degree of integration of security elements in the context of dynamic digital modernisation. The relevance of this approach was confirmed in the present study, which recorded the dependence of the effectiveness of incident response on the level of coordination of security policies at the cross-functional level.

The study found that the lack of clearly defined risk management strategies and weak institutional responsibility between departments negatively affected the effectiveness of response measures. This aspect was revealed by Nowicka et al.[41], who identified barriers to security management in the context of digital transformation, specifically, the fragmentation of functional interaction. The researchers noted that reorganisation with a focus on transparency and accountability between departments reduces the average incident response time by 35-42%, which was consistent with the results of the current analysis.

---

39 H. HOKMABADI, S.M. REZVANI and C.A. DE MATOS, *Business resilience for small and medium enterprises and startups by digital transformation…*, in *Systems*, 2024, 12(6), p. 220.

40 G.S. LAMPE, *Critical success factors for integrating a circular interaction model for security processes in digital transformation*, in *Ecoforum Journal*, 2023, 12(2), p. 1.

41 J. NOWICKA, Z. CIEKANOWSKI, J. KUDINS and P.J. D□BROWSKI, *Managing organizational security in the era of digital transformation*, in *European Research Studies Journal*, 2024, 27(3), pp. 460–471.

The economic context of digital security revealed further aspects of the relationship between the institutional sensitivity of enterprises to risks and the effectiveness of digital adaptation[42]. Samoilenko et al.[43] emphasised that ensuring economic security in the context of digitalisation is possible only if technological, anti-crisis, and strategic tools are synergised. The findings obtained in the present study confirmed the relevance of this approach, particularly for medium-sized businesses, where the level of digital readiness is often combined with limited resources.

The use of Information Security Management Systems proved to be critical to reducing the vulnerability of enterprises in high-risk industries[44]. Jonathan et al.[45] empirically proved that the implementation of ISO/IEC 27001 standards ensures the integration of IT infrastructure and reduces the number of critical vulnerabilities by 27%. The analysis confirmed the effectiveness of such systems, especially in countries with a unified regulatory framework for cybersecurity.

The issue of the human factor continues to be a significant barrier to cyber resilience, especially in organisations in the early stages of digital transformation[46,47]. Stewart[48] noted that over 42% of information security breaches were caused by human error or insufficient staff training. The data obtained in the present study confirmed the existence of a direct correlation between the covera-

---

42 M. KNAPIK, *Analysis of water leaks and savings strategies in commercial buildings and the impact of LEED certification on water system operating cost*, in *Zeszyty Naukowe SGSP*, 2025, 1(95), pp. 41–58.

43 Y. SAMOILENKO, I. BRITCHENKO, I. LEVCHENKO, P. LOSONCZI, O. BILICHENKO and O. BODNAR, *Economic security of the enterprise…*, in *Economic Affairs*, 2022, 67(4), pp. 619–629.

44 E. DAHAN, I. AVIV and M. KIPERBERG, *Trust domain extensions guest fuzzing framework for security vulnerability detection*, in *Mathematics*, 2025, 13(11), p. 1879.

45 G.M. JONATHAN, E. PERJONS and L. RUSU, *Untangling the link between digital transformation and information security management*, in *Procedia Computer Science*, 2024, 239, pp. 575–582.

46 D. PAVLOVA, T. DOVRAMADJIEV, D. DASKALOV, N. MIRCHEV, I. PEEV, J. RADEVA, R. DIMOVA, K. KAVALDZHIEVA, B. MRUGALSKA, G. SZABO and A. KANDIOGLOU, *3D design of a dental crown with artificial intelligence based in cloud space*, in *Lecture Notes in Networks and Systems*, 2024, 817, pp. 437–445.

47 N. KIKTEV, O. VASYLENKO, I. HORETSKA, A. PANCHENKO, S. SLOBODIAN, M. KUBOŃ, Z. SKIBKO and T. HUTSOL, *Smart solutions in agricultural robotics*, in *Agricultural Engineering*, 2025, 29(1), pp. 157–186.

48 H. STEWART, *Digital transformation security challenges*, in *Journal of Computer Information Systems*, 2023, 63(4), pp. 919–936.

ge of employees with cybersecurity programmes and a decrease in the frequency of incidents, which is consistent with the conclusions set out in the cited study.

The analysis of the study findings revealed that the systemic problem of a shortage of digital skills in the field of information security significantly limited the resilience of organisations to the growing threats of the digital environment. It was found that even in countries with high levels of institutional maturity, there was significant variation in the level of digital training of staff, which complicated the unification of response strategies. This conclusion correlates with the results of a systematic review by Ruoslahti et al.[49], who highlighted the chronic mismatch between academic training programmes and practical market requirements for cyber skills. Within the framework of this study, this problem was manifested in the specific features of the HR policy of small and medium-sized businesses, which, due to a lack of internal expertise, could not provide effective counteraction to threats even with basic technological tools.

An analysis of the digital architecture of organisational security showed that the functioning of sustainable partnership networks plays a key role in minimising the consequences of cyber incidents, especially in conditions of limited institutional support. Trim and Lee[50] proved that the global partnership model, which integrates technical solutions, political support, and inter-organisational interaction, is an effective mechanism for countering large-scale attacks. The study confirmed the relevance of this concept, demonstrating that in countries with an average level of regulatory readiness, partnership mechanisms made it possible to compensate for the fragmentation of the legislative field and insufficient resources.

The key factor in improving the effectiveness of cyber defence at enterprises with a developed digital infrastructure was the presence of strategic leadership in the field of information security[51,52]. Al-Kumaim and Alshamsi[53] found that the active position of leaders in implementing cybersecurity policies reduced risks

49 H. RUOSLAHTI, J. COBURN, A. TRENT and I. TIKANMAKI, *Cyber skills gaps: A systematic review…*, in *Connections: The Quarterly Journal*, 2021, 20(2), pp. 33–45.

50 P.R. TRIM and Y.I. LEE, *The global cyber security model…*, in *Big Data and Cognitive Computing*, 2021, 5(3), p. 32.

51 S. PORKODI, *The effectiveness of agile leadership in practice: A comprehensive meta-analysis of empirical studies on organizational outcomes*, in *Journal of Entrepreneurship Management and Innovation*, 2024, 20(2), pp. 117–138.

in critical sectors, including the financial sector. The findings showed that in countries with a prominent level of digital maturity, where cyber risk management functions are clearly institutionalised, the effectiveness of incident response increased and the average response time to a breach decreased.

In the context of escalating cyber threats, adaptive countermeasures that combine proactive forecasting and reactive response mechanisms became particularly significant. Safitra et al.[54] proposed a conceptual framework that combined preventive, adaptive, and reactive tools within a single digital security architecture. An analysis of the strategic documents of the countries covered by the study revealed analogous approaches to digital policy formation, particularly in terms of implementing mechanisms for multi-level interaction between the state, corporate, and technical levels.

The development of a sustainable cybersecurity culture was viewed as one of the fundamental areas of ensuring the digital resilience of organisations in the face of increasing information flows[55]. Aksoy[56] provided statistical evidence that systematic staff training, development of incident protocols, and regular internal training directly correlated with the level of prevention of both external and internal threats. The study found that these measures were particularly relevant for small businesses, which typically have limited resources to implement complex technical systems but can compensate for this by paying closer attention to human capital.

Within the framework of the assessment of SMEs' readiness to implement digital security protocols, the study analysed an application guide developed by

---

52 S. PORKODI and A. M. RAMAN, *Success of cloud computing adoption over an era in human resource management systems: A comprehensive meta-analytic literature review*, in *Management Review Quarterly*, 2025, 75(2), pp. 1041–1075.

53 N.H. AL-KUMAIM and S.K. ALSHAMSI, *Determinants of cyberattack prevention in UAE financial organizations: Assessing the mediating role of cybersecurity leadership*, in *Applied Sciences*, 2023, 13(10), p. 5839.

54 M.F. SAFITRA, M. LUBIS and H. FAKHRURROJA, *Counterattacking cyber threats: A framework…*, in *Sustainability*, 2023, 15(18), p. 13369.

55 V.A. KRASNOBAYEV, S.A. KOSHMAN and M.A. MAVRINA, *A method for increasing the reliability of verification of data represented in a residue number system*, in *Cybernetics and Systems Analysis*, 2014, 50(6), pp. 969–976.

56 C. AKSOY, *Building a cyber security culture for resilient organizations against cyber attacks*, in *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, 2024, 7(1), pp. 96–110.

Papathanasiou et al.[57], which sets out recommendations for adapting security infrastructure in a low-finance environment. The study confirmed that the lack of clearly structured procedures and regulatory uncertainty continue to be critical barriers for SMEs in the context of increased vulnerability to external attacks. Of particular relevance is the creation of sectoral programmes to support small businesses in cyber defence, which include both technological solutions and training and advisory mechanisms adapted to the specifics of the business environment[58].

Particular attention was paid to the impact of digital integration on the efficiency of business structures in transforming economies. The findings of the study were consistent with those of Alog et al.[59], who proved that digital integration was one of the key drivers of the operational sustainability of small enterprises, especially in conditions of limited access to capital and technological resources. In their analysis, analogous trends were recorded in Albania and Croatia, where digital integration was accompanied by an increase in the share of e-commerce in the GDP.

Al-Dosari and Fetais[60] conducted a meta-analysis of risk management and information security systems used by SMEs. The researchers found that the effectiveness of the use of the relevant systems largely depended on the availability of comprehensive risk management strategies adapted to the limited resources of small enterprises. The present study confirmed the relevance of this model, especially in the cases of Estonia and the Czech Republic, where enterprises implemented adaptive digital security frameworks.

The issue of structural barriers to digital transformation in SMEs was also confirmed by Rupeika-Apoga and Petrovska[61], who identified a lack of digital

57 A. PAPATHANASIOU, G. LIONTOS, A. KATSOURAS, V. LIAGKOU and E. GLAVAS, *Cybersecurity guide for SMEs*…, in *Journal of Information Security*, 2024, 16(1).

58 A. SADENOVA, O. DENISSOVA, M. KOZLOVA, S. RAKHIMOVA, A. GOLA and S. SUIEUBAYEVA, *Structural equation modeling (SEM) in jamovi: An example of analyzing the impact of factors on enterprise innovation activity*, in *Applied Computer Science*, 2025, 21(1), pp. 97–110.

59 K. ALOG, K. ATIYA, R. SENTANI and M. ALKHATTALI, *Impact of digital integration on the small and medium-sized enterprises in Arab countries*, in *Afro-Asian Journal of Scientific Research*, 2025, 3(1), pp. 41–54.

60 K. AL-DOSARI and N. FETAIS, *Risk-management framework and information-security systems for small and medium enterprises (SMES): A meta-analysis approach*, in *Electronics*, 2023, 12(17), p. 3629.

61 R. RUPEIKA-APOGA and K. PETROVSKA, *Barriers to sustainable digital transformation*…, in *Sustainability*, 2022, 14(20), p. 13558.

competencies, insufficient funding, and fragmented regulatory support as key factors hindering transformation. Analogous limitations were recorded in Albania, suggesting the need for more support from the state and the expansion of digital adaptation programmes.

The value of digital integration for the participation of enterprises in global value chains was confirmed by Vu et al.[62]. In the present study, analogous dependencies were established on the example of Croatia and Lithuania, where the growth of digital maturity was directly correlated with the expansion of the presence of enterprises in foreign markets. This helped to consider digital transformation not only as a security tool but also as a platform for strategic growth.

The analysis revealed the existence of stable correlations between the level of digital maturity, the spread of cybersecurity tools, and the effectiveness of responding to digital risks, which is manifested in reducing the frequency of critical incidents and increasing the overall resilience of the information infrastructure of enterprises. The study established that the integration of technological solutions (specifically, Security Information and Event Management and Endpoint Detection and Response systems), regulatory instruments (national cybersecurity strategies, data protection regulations), and organisational practices (staff training, information security culture, inter-institutional interaction) creates preconditions for reducing economic losses and ensuring faster recovery from cyber incidents. The totality of the identified dependencies indicates the need for a holistic approach to the development of digital security, based on a systematic combination of technological modernisation, institutional development and improvement of human capital. The findings are conceptually consistent with modern scientific approaches to cyber risk management, particularly those that emphasise the significance of multi-level interaction in the digital environment.

5. Conclusions

The present study showed a prominent level of dependence between digital competences, institutional security measures, and the economic resilience of national economies to cyber threats. Based on a comparative analysis of five

62 N.H. VU, T.A. BUI, T.B. HOANG and H.M. PHAM, *Information technology adoption and integration into global value chains: Evidence from small-and…*, 2022.

countries – Albania, Croatia, Czech Republic, Estonia, and Lithuania – the study found that the highest digital maturity indicators were observed in Estonia (74.3 according to the Digital Economy and Society Index), the Czech Republic (69.2), and Lithuania (59.8), which correlated with a greater share of e-commerce in GDP – up to 9.8% in the Czech Republic and 8.6% in Estonia. The analysis of statistics also confirmed that prominent levels of corporate cyber awareness coverage (up to 81% in Estonia) were accompanied by lower productivity losses and better recovery dynamics after incidents. The greatest levels of Digital Skills Indicator were recorded in Estonia (72.1) and the Czech Republic (66.5), which coincided with the highest Human Capital Index values (0.79 and 0.75, respectively).

The results also revealed a strong correlation between the use of key security technologies (specifically, Security Information and Event Management and Endpoint Detection and Response) and the reduction of the negative impact of digital incidents on business operations. Countries with a high adoption rate of cloud services, multi-level authentication, and event monitoring systems (up to 76% in Estonia) had a significantly lower burden of incidents and financial losses on SMEs. For instance, while Albania recorded 157 incidents in the small business sector, the greatest average losses were incurred by Estonia (EUR 6.7 mn), indicating vulnerability at a high level of digital integration. At the same time, the Czech Republic demonstrated the lowest probability of losing solvency (0.33), which indicated the effectiveness of institutional measures and the implementation of certified solutions.

A generalisation of the e-Government Development Index and Global Cybersecurity Index indicators showed an increase in the regulatory readiness of all countries in 2024-2025, specifically in Albania from 0.694 to 0.712 according to the e-Government Development Index. The study found that countries with high human capital indices, such as the Czech Republic and Estonia, had advantages in reducing incidents, shorter business interruption periods, and stable macroeconomic indicators. This demonstrates the effectiveness of integrating digital education and corporate cyber culture into digital transformation policies. A limitation of the present study was the limited access to microdata on corporate cybersecurity practices and the lack of unified

indicators to assess the effects of digital technologies on the financial and logistical stability of enterprises. Prospects for further research include modelling industry-oriented digital security structures and analysing mechanisms to stimulate cyber resilience in small businesses and the public sector.