INTERNATIONAL JOURNAL OF POLITICAL SCIENCES AND ECONOMICS
Impact Factor (research bib) - 9,78
https://ijmri.de/index.php/ijpse , German international journals company
ISSN 2751-9708

A MODEL OF CYBERSECURITY, LEGAL LIABILITY, AND INSTITUTIONAL STABILITY IN ELECTRONIC COMMERCE SYSTEMS BASED ON ARTIFICIAL INTELLIGENCE

Danayeva Zulhumor Abdusodiq kizi

Samarqand iqtisodiyot va servis institutitalabasi

ORCID 0009-0005-4414-203X

danayevazulhumor275@gmail.com

Abstract: The deep integration of artificial intelligence (AI) technologies into global e-commerce platforms has significantly optimized operational processes, expanded the scope of cybersecurity risks and formed new digital attack vectors. In this context, the need for a comprehensive analysis of the interrelationship between cybersecurity, legal accountability, and institutional stability is growing. This study develops an AI-CLIS (Artificial Intelligence Cybersecurity–Legal Accountability–Institutional Stability) model that integrates these three components. The model analyzes the impact of AI governance on security and institutional stability in e-commerce ecosystems based on a multidimensional approach.

Keywords: artificial intelligence security; e-commerce cybersecurity; institutional stability; legal accountability; digital trust; AI governance; adversarial machine learning; panel data analysis; digital policy of Uzbekistan.

Annotatsiya: Sun’iy intellekt (SI) texnologiyalarining global elektron tijorat platformalariga chuqur integratsiyasi operatsion jarayonlarni sezilarli darajada optimallashtirgan holda, kiberxavfsizlikka oid xavf-xatarlar doirasini kengaytirdi hamda yangi raqamli hujum vektorlarini shakllantirdi. Ushbu sharoitda kiberxavfsizlik, huquqiy javobgarlik va institutsional barqarorlik o‘rtasidagi o‘zaro bog‘liqlikni kompleks tarzda tahlil qilish zarurati ortib bormoqda. Mazkur tadqiqot ushbu uch komponentni integratsiya qiluvchi AI-CLIS (Artificial Intelligence Cybersecurity–Legal Accountability–Institutional Stability) modelini ishlab chiqadi. Model elektron tijorat ekotizimlarida sun’iy intellekt boshqaruvining xavfsizlik va institutsional barqarorlikka ta’sirini ko‘p o‘lchovli yondashuv asosida tahlil qiladi.

Kalit so‘zlar: sun’iy intellekt xavfsizligi; elektron tijorat kiberxavfsizligi; institutsional barqarorlik; huquqiy javobgarlik; raqamli ishonch; AI boshqaruvi; adversarial mashinani o‘rganish; panel ma’lumotlar tahlili; O‘zbekiston raqamli siyosati.

Аннотация: Глубокая интеграция технологий искусственного интеллекта (ИИ) в глобальные платформы электронной коммерции значительно оптимизировала операционные процессы, расширила масштабы рисков кибербезопасности и сформировала новые векторы цифровых атак. В этом контексте возрастает потребность в всестороннем анализе взаимосвязи между кибербезопасностью, правовой ответственностью и институциональной стабильностью. В данном исследовании разработана модель ИИ-КИБ (Кибербезопасность на основе искусственного интеллекта – Правовая ответственность – Институциональная стабильность), которая объединяет эти три компонента. Модель анализирует влияние управления ИИ на безопасность и институциональную стабильность в экосистемах электронной коммерции на основе многомерного подхода.

INTERNATIONAL JOURNAL OF POLITICAL SCIENCES AND ECONOMICS
Impact Factor (research bib) - 9,78
https://ijmri.de/index.php/ijpse , German international journals company
ISSN 2751-9708

Ключевые слова: безопасность искусственного интеллекта; кибербезопасность электронной коммерции; институциональная стабильность; правовая ответственность; цифровое доверие; управление ИИ; состязательное машинное обучение; анализ панельных данных; цифровая политика Узбекистана.

INTRODUCTION

The global e-commerce market is estimated to be worth approximately US$5.8 trillion in 2023 and is projected to exceed US$8.1 trillion by 2026. The key technological drivers of this growth are artificial intelligence (AI) systems—recommendation algorithms, fraud detection models, dynamic pricing mechanisms, and automated customer services—that are directly reshaping the operational and competitive structure of e-commerce.[1]

At the same time, the expansion of AI-based systems has also exposed new systemic vulnerabilities. According to a report by the World Economic Forum, AI-based cyberattacks are listed as one of the top three threats to global economic stability. ENISA (2024) data shows that cyberattacks targeting AI increased by 340% between 2021 and 2024, with 38% of these attacks targeting e-commerce platforms. This means that existing traditional cybersecurity approaches are not fully adapted to the SI environment. Along with the widespread use of SI technologies in e-commerce, the economic scale of cybercrime has also increased significantly. According to FBI IC3 (2024), in 2023, cybercrime losses in the United States alone were recorded at $12.5 billion, of which 31.4% were due to e-commerce fraud. Globally, Cybersecurity Ventures predicts that the annual economic loss of cybercrime will reach $10.5 trillion by 2025. This figure makes cybercrime one of the largest generators of damage to the global economy. In particular, adversarial machine learning techniques pose a direct threat to cybersecurity systems. Techniques such as evasion attacks, data poisoning, and model extraction allow to defeat SI-based fraud detection systems. Research by Biggio and Roli (2018) shows that these attacks, even when they are imperceptible to human perception, can lead to serious errors in classification systems. Apruzzese et al. (2022) empirically confirm that 67% of application systems are vulnerable to adversarial attacks. Cybersecurity problems are not limited to financial losses; they lead to a systemic erosion of digital trust. Research by Gefen and McKnight (2003; 2011) shows that trust is a key determinant of online transactions. A decrease in trust among participants directly leads to a decrease in the intensity of platform use. According to Eurostat (2024), 47% of users have reduced the frequency of online purchases on platforms where data breaches have occurred, and 23% have abandoned these platforms altogether. The ITU Global Cybersecurity Index (2024) notes a strong negative correlation between the level of cybersecurity incidents and the development of e-commerce ($r = -0.61$, $p<0.001$). Institutional weakness is one of the main factors that exacerbate these processes. According to the approaches of North (1990), Rodrik (2004) and Acemoglu & Robinson (2012), weak institutions increase transaction costs and reduce economic efficiency. In the SI-based e-commerce environment, this creates “governance vacuums”, that is, situations where the pace of technological development exceeds the capacity of institutional regulation.

Uzbekistan is considered an important empirical model in terms of digital transformation processes. E-commerce and digital services have expanded significantly under the Digital Uzbekistan 2030 strategy and the Law on Personal Data. According to the Agency for Statistics of the Republic of Uzbekistan and the United Nations Development Program, the level of e-commerce use increased from 12% to 34% between 2019 and 2024. At the same time, data from the State Information Security Inspectorate shows that the number of cyber incidents increased by 287% between 2021 and 2023, the bulk of which fell on e-commerce platforms. However, the

current institutional framework does not fully cover the risks posed by IS. The national cybersecurity strategy does not contain clear regulatory mechanisms for adversarial attacks on IS, algorithmic liability, and cross-border data management. According to the ITU index, Uzbekistan ranks 62nd, maintaining relatively low indicators in terms of legal measures and institutional capacity.

Literature review

Since 2019, scientific research on artificial intelligence-based cybersecurity in the e-commerce environment has expanded significantly. The initial theoretical foundations were formulated by Sommer and Paxson, who identified the problem of "distributional shift" in intrusion detection systems based on machine learning - that is, the difference between training and practical environments - as a key weakness[2]. The classification of adversarial attacks (exploratory and causative attacks) developed by Barreno et al. is still used as a methodological basis in AI security research today. In subsequent works, this approach has been expanded, and adversarial threats are now considered not only as technical, but also as systemic risks[3].

In the normative direction, Floridi et al. define security as one of the five key components of AI governance. The NIST AI Risk Management Framework has transformed this approach into a practical standard, defining structural mechanisms for identifying and managing risks in AI systems. These documents provide a basis for interpreting AI cybersecurity as a system that is inextricably linked to institutional governance, rather than an independent technical issue[4]. While empirical studies confirm the effectiveness of AI-based fraud detection systems, their robustness directly depends on the quality of platform architecture and data management. At the same time, adversarial trained models require high computational costs, which creates operational limitations in real-time transactional environments[5]. The issue of legal liability for decisions based on AI is one of the central areas of modern digital law. Doshi-Velez et al. define algorithmic liability through three main components-explanation, justification, and oversight.[6] However, the "liability gap"-the gap between the harm caused by AI and legal liability-remains a major problem in the academic literature. Schaerer et al. explain this situation by three factors: algorithmic "opacity," emergent behavior, and the distributed nature of decision-making. As a result, there are significant differences between liability approaches across jurisdictions, creating a risk of regulatory arbitrage for global e-commerce platforms.[7]

Digital trust is a key institutional resource in e-commerce systems. Based on the approaches of Mayer et al., Williamson and North, trust is interpreted as a key factor that reduces transaction costs. McKnight and Chervany have separated digital trust into cognitive and behavioral components and identified its direct impact on online transactions. Pavlov has integrated trust with the technology acceptance model to form an empirically based measurement system in the e-commerce environment.[8],[9]

Recent research shows that AI systems complicate the dynamics of trust. Gillath et al. have found that overconfidence in AI leads to a sharp loss of trust after its errors. Hancock et al. have empirically confirmed that the effectiveness of human-AI cooperation is maximized at an optimal level of trust.[10] Cybersecurity breaches significantly reduce trust levels, and this effect leads to long-term behavioral changes. ITU data show that there is a strong statistical relationship between the level of national cybersecurity and the development of e-commerce.

The analysis shows that the existing scientific literature has developed in three independent directions: technical cybersecurity, legal liability, and institutional governance. However, since

these directions have developed without mutual integration, the ability to fully assess complex risks in AI-based e-commerce systems is limited. It is this gap that justifies the need to develop an AI-CLIS model, since existing approaches provide technical accuracy or institutional breadth separately, but do not combine them in a single analytical framework.

Methodology

The empirical analysis is based on an unbalanced panel database formed for 11 jurisdictions between 2021 and 2025. The total number of observations is a maximum of 55 jurisdiction-year units. The jurisdictions included in the analysis were selected according to the criteria of institutional quality, degree of digitization, intensity of implementation of artificial intelligence technologies, and geographical diversification. The sample consists of three main groups: highly institutionally developed economies (USA, EU, UK, South Korea, Singapore), rapidly developing digital economies (China, India, UAE) and transition economies (Turkey, Kazakhstan, Uzbekistan).

Eurostat ICT Usage Survey microdata were used for the European Union, and equivalent national statistical surveys were used for other jurisdictions. Missing observations were replaced by multiple imputation based on the EM algorithm, and the stability of the results was confirmed by sensitivity analyses. Four main composite indices were developed within the framework of the study: AI Cybersecurity Index for Commerce, Legal Liability and Compliance Index, Institutional Stability Index and Digital Trust and Resilience Index. The formation of the indices was carried out based on a two-stage approach. In the first stage, all indicators were standardized across the entire panel (z-score transformation) and aggregated based on equal weights for internal subcomponents. In the second stage, statistical weights were determined through principal component analysis (PCA), components meeting the eigenvalue>1 criterion were retained, and varimax rotation was applied.

Discussion and Results

The table below presents the standardized averages of the five main composite indices of the AI-CLIS model—the AI Cybersecurity Index for Commerce (AICI), the Legal Liability & Compliance Index (LLCI), the Institutional Stability Index (ISI), the Digital Trust & Resilience Index (DTRI), and the Platform Resilience Index (PRI)—for 11 jurisdictions. These indices are aggregated based on panel data from 2021–2025, with each index representing a country's level of technical, legal, and institutional readiness in a unified measurement system. The table allows for cross-jurisdictional heterogeneity to be identified and resilience determinants to be compared in AI-enabled e-commerce ecosystems to be compared.

Table 1:

Summary statistics of the cross-jurisdictional index (panel averages from 2021–2025)

Jurisdiction	AICI (Cybersecurity)	LLCI (Legal Compliance)	ISI (Institutional Stability)	PRI (Platform Resilience Index)
United States	1.41	1.36	1.38	1.42
European	1.52	1.58	1.53	1.55

Union				
United Kingdom	1.32	1.28	1.34	1.32
China	0.66	0.44	0.58	0.66
Singapore	1.56	1.60	1.55	1.57
South Korea	1.24	1.22	1.20	1.22
United Arab Emirates	0.91	0.88	0.92	0.91
India	0.36	0.34	0.38	0.36
Turkey	0.14	0.12	0.13	0.13
Kazakhstan	-0.45	-0.47	-0.44	-0.45
Uzbekistan	-0.46	-0.44	-0.52	-0.46

The results of the table show that there are significant structural differences across jurisdictions in three key layers of the AI-driven digital economy – technological cybersecurity (AICI), legal regulation (LLCI) and institutional stability (ISI). The highest overall resilience profile is recorded by Singapore (PRI=1.57) and the European Union (PRI=1.55), which indicates a synchronous development of high AICI, LLCI and ISI values.

While the US (PRI=1.42) and the UK (PRI=1.32) have high technological maturity, their index dynamics show relatively strong, but not fully symmetrical integration with legal and institutional components. South Korea (PRI=1.22) and the UAE (PRI=0.91) are located in the medium-high cluster, indicating that technological development is slightly faster than legal and institutional adaptation.

China (PRI=0.66) has a relatively high technological cybersecurity (AICI=0.87) but a low legal accountability index (LLCI=0.44), indicating a limited overall level of resilience. This structure reflects the phenomenon of "technology-regulation mismatch".

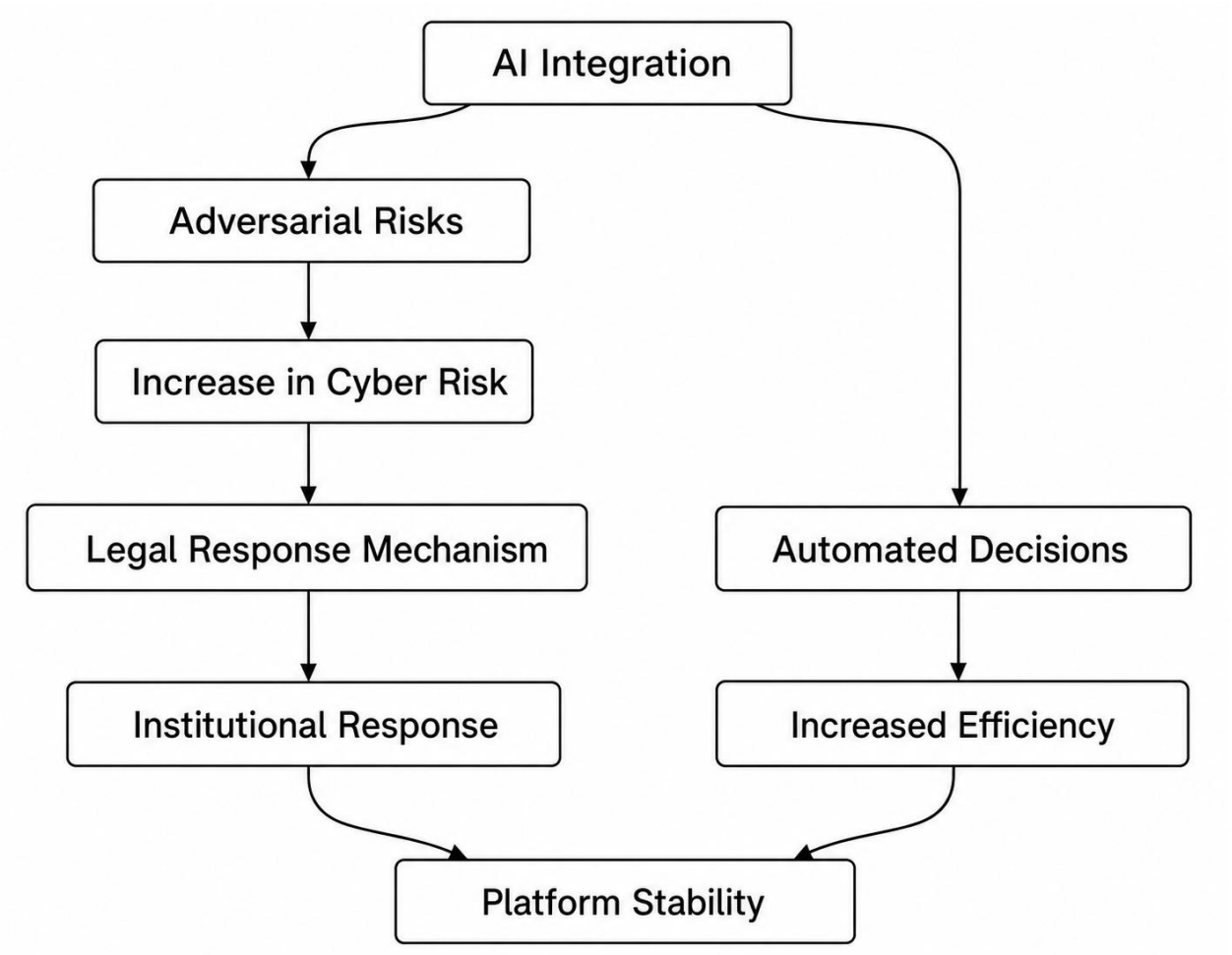
India (PRI=0.36) and Turkey (PRI = 0.13) are located in the low-medium cluster, indicating insufficient synchronous development between the three main components – technical, legal and institutional – in these jurisdictions.

Kazakhstan (PRI =-0.45) and Uzbekistan (PRI =-0.46) form the lowest cluster. The simultaneous low values of AICI, LLCI and ISI in these jurisdictions indicate a systemic limitation of platform resilience. In particular, in Uzbekistan, the ISI (-0.52) and LLCI (-0.44) indicators confirm that the institutional and legal layers have not developed in line with the pace of implementation of AI technologies. In general, the results empirically confirm that AI-based e-commerce resilience is formed not by individual technological factors, but by the joint synchrony of technical (AICI), legal (LLCI) and institutional (ISI) components. In this regard, the PRI indicator is interpreted as an aggregated expression of the level of balance between these

three layers. The results of the empirical assessment show a strong and statistically stable relationship between the technical, legal and institutional components formulated within the AI-CLIS model and platform resilience. The overall regression results confirm that AI cybersecurity maturity, legal accountability mechanisms and the quality of institutional governance are the main determinants of the resilience of e-commerce systems. AI cybersecurity maturity has a positive and high significance level in all specifications, and its increase leads to a significant increase in platform resilience. This result suggests that AI-based security infrastructure is not just a technical protection tool, but also a key factor shaping systemic economic stability. The effect size is practically significant and is associated with a significant reduction in cyber fraud losses.

Figure 1

A causal (mechanistic) model between cybersecurity, legal liability, and institutional stability in e-commerce based on AI



Legal accountability and enforcement effectiveness are also identified as independent and stable determinants. This result shows that no matter how high the level of technical security is, if legal institutions are weak, the overall platform resilience will not be fully formed. In particular, in transition economies, the marginal impact of the legal component is higher, which

is explained by the fact that these institutions are in the development stage. The interaction dependencies in the model clearly confirm institutional complementarity. The effectiveness of AI cybersecurity investments increases significantly under conditions of high institutional governance quality. This indicates the existence of a synergistic relationship between technological investments and the institutional environment. At the same time, the joint effect of the data protection system and legal accountability mechanisms is also of a reinforcing nature, and they work not separately, but as a whole "institutional ecosystem". The results of the dynamic panel estimation are fully consistent with the main model and confirm the validity of the instrumental variables. This strengthens the causal interpretation of the presented results and confirms the econometric stability of the model. The results of the subsample analysis show that there are clear structural differences between developed and developing economies. While the impact of AI cybersecurity maturity is stronger in developed economies, the impact of legal institutions is of relatively high marginal importance in developing economies. This reflects the asymmetry of technological and institutional development stages. The results of the structural equation model strengthen the theoretical validity of the empirical model. The model fit indices are high, confirming the strong coherence between the observed data and the theoretical framework. The results indicate that AI cybersecurity investments do not directly affect digital trust, but mainly indirectly through institutional governance. At the same time, the legal accountability system is identified as one of the strongest direct determinants of digital trust. The results of the measurement model confirm a high level of validity across all constructs. The constructs are mutually differentiated and statistically independent, which empirically substantiates the multidimensional structure of the AI-CLIS model.

The diagnostic analysis for Uzbekistan shows that the country's digital economy is dominated by transitional features. While the technical cybersecurity infrastructure is well-established, the institutional and legal components are relatively lagging behind. This imbalance is a key factor determining the low level of platform resilience. The results of the counterfactual assessment show that if a developed regulatory system and enforcement mechanisms for data protection were introduced in Uzbekistan at an early stage, digital trust and platform resilience would be significantly higher. This difference is also economically significant and indicates the possibility of preventing a significant part of the losses associated with cybersecurity. The empirical results confirm the systemic nature of the interrelationship between cybersecurity, legal regulation and institutional stability in AI-based e-commerce ecosystems. In this regard, the integrated regulatory architecture of the European Union stands out as the most developed governance model at the global level. In the EU, the institutional coherence between the NIS2 Directive, the Cybersecurity Act and the AI Act forms a multi-layered regulatory framework that combines technical security requirements with legal obligations. The key feature of this approach is that it covers not only cybersecurity, but also the behavioral and functional risks of AI systems. Empirical results show that the EU has the highest LLCI and DTRI indicators, confirming the practical effectiveness of this regulatory model. At the same time, the European model is not without internal coordination problems. The divergence of enforcement mechanisms between Member States creates regulatory fragmentation at the level of the single market. In addition, high compliance costs for small and medium-sized businesses can affect the competitive balance.

And extraterritorial use increases enforcement complexity for global platforms. The United States model was formed as a market-based approach, relying mainly on ex-post liability. While this model encourages an innovative environment, it creates inconsistencies in the level of legal compliance due to regulatory fragmentation. The results show that the USA has a high level of

AICM but a relatively low level of LLCI, which represents a structural gap between technical innovation and legal stability.

The Singaporean model stands out as a small-scale but high-efficiency institutional design. Empirical results confirm that a proactive and principled regulatory approach can achieve high institutional efficiency even in resource-limited conditions. A particularly high level of the ISI indicates an optimal balance between the quality of institutional governance and performance in Singapore. Although the Chinese model is normatively strong, a significant difference between de jure and de facto regulation remains due to the presence of selectivity in enforcement practice. This situation reduces legal certainty and increases the level of uncertainty for market participants. As a result, the high technological cyber security potential cannot be translated into full institutional effectiveness.

The results for Uzbekistan and general transition economies show the existence of a structural "gap" in digital management systems. This difference is interpreted not only as a technological problem, but also as a systemic problem related to institutional and resource distribution. Empirical assessment shows that the AI-CLIS components of Uzbekistan are significantly lower than the average value, which means that the institutional foundations of resilience are not yet fully formed. This disparity is explained by three main mechanisms. First, there is a temporal mismatch between technological development and institutional regulation, and the speed of the digital economy is faster than the speed of adaptation of regulatory systems. Second, the lack of specialized personnel limits the effectiveness of AI governance and cybersecurity regulation. Thirdly, institutional fragmentation reduces the level of coordination between different state bodies and reduces the efficiency of general management.

Through comparative analysis, this problem is not unique to Uzbekistan. It can be said that a similar structural imbalance is observed in middle-income economies such as Kazakhstan, Turkey, and India. This means that there is a systemic phenomenon that can be called "middle-income governance gap" in the development of the digital economy. The results show that stability in AI-based e-commerce systems is determined not only by technological investments, but also by institutional maturity and legal certainty. Therefore, future political approaches should be focused on joint development of regional coordination and institutional capacity, in addition to individual state level.

Conclusions and recommendations

The conceptual basis of the model is formed by five main principles: a risk-based regulatory approach, the principle of technological neutrality, institutional continuity, regional coordination mechanisms and an adaptive governance system. These principles ensure that the regulatory system is not static, but dynamic and evolutionary. For transitional economies, in particular Uzbekistan, the most priority is the formation of a legal accountability system based on AI. Empirical results show that the level of legal certainty is one of the strongest determinants of digital trust and platform resilience. In this regard, AI systems used in the e-commerce sector should be classified as high-risk systems. This is based on their role in payment systems, identification and fraud detection processes. For high-risk systems, it is necessary to strengthen the manufacturer's liability, partially shift the burden of proof to operators, and introduce a mandatory incident reporting system.

For Uzbekistan, it is advisable to implement legal transformation in three stages. The first stage involves aligning personal data protection legislation with international standards, the

second stage involves adopting a separate AI governance law, and the third stage involves implementing a strategy to achieve "adequacy" status on data flows with the European Union. Empirical results show that institutional weakness is the main limiting factor for AI governance. Therefore, the ACIS-2035 model proposes developing institutional capacity in two directions: staff quality and institutional integration. The first direction involves creating a specialized training system for AI governance. This system will be formed in cooperation with universities, government agencies, and international organizations and will focus on training specialists at the intersection of cybersecurity, law, and the data economy. The second direction involves the formation of a centralized cybersecurity and AI monitoring center. This will increase operational efficiency by integrating existing fragmented systems and allow for real-time threat detection. It is also recommended to expand regulatory "sandbox" mechanisms. This approach allows new technologies to be tested in real-world, but controlled, conditions, increasing regulators' ability to learn adaptively. Empirical estimates suggest that these investments generate significant economic returns in the medium term. Significant fiscal and economic benefits arise from reduced cyber fraud losses, increased digital trust, and increased e-commerce. In particular, increased digital trust has a direct impact on e-commerce activity. This study analyzed the relationship between cybersecurity, legal accountability, and institutional stability in AI-based e-commerce systems using an integrated empirical model. The AI-CLIS model integrates technical, legal, and institutional factors into a single analytical framework. The results show that AI cybersecurity maturity is the main technical determinant of platform resilience, but its full impact is enhanced by the quality of institutional governance. The legal accountability system is identified as the strongest direct determinant of digital trust.

The empirical assessment showed significant differences across 11 jurisdictions, confirming that these differences are explained more by institutional maturity than by technological development. In particular, in transition economies, a structural imbalance between technological development and regulatory institutions was found. The diagnostic analysis for Uzbekistan showed that institutional and legal components lag behind in the development stage of the digital economy. The results of the counterfactual assessment confirmed that significant economic losses can be avoided if appropriate regulatory systems are introduced. Future research should be directed towards regional expansion of this model, the development of real-time monitoring systems, and the implementation of micro-empirical analyses at the firm level. This will further deepen the theoretical and practical integration in the field of AI governance.

References:

1. Acemoglu, D., & Robinson, J. A. (2012). Why Nations Fail: The Origins of Power, Prosperity, and Poverty. Crown Business.
2. Apruzzese, G., Pierazzi, F., Colajanni, M., & Marchetti, M. (2022). Detection and adversarial machine learning in cybersecurity: A survey. ACM Computing Surveys, 54(6), 1–36.
3. Bertrand, M., Duflo, E., & Mullainathan, S. (2004). How much should we trust differences-in-differences estimates? Quarterly Journal of Economics, 119(1), 249–275.
4. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317–331.
5. ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity.
6. European Union. (2024). Artificial Intelligence Act (Regulation 2024/1689).
7. European Union. (2022). NIS2 Directive (Directive 2022/2555).
8. European Union. (2019). Cybersecurity Act (Regulation 2019/881).
9. Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables. Journal of Marketing Research, 18(1), 39–50.

10. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping. MIS Quarterly, 27(1), 51–90.
11. Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis. Structural Equation Modeling, 6(1), 1–55.
12. McKinsey Global Institute. (2023). The economic potential of generative AI.
13. OECD. (2019/2024). Recommendation on Artificial Intelligence. OECD Publishing.
14. OECD. (2023). Going Digital Toolkit. OECD Publishing.
15. North, D. C. (1990). Institutions, Institutional Change and Economic Performance. Cambridge University Press.
16. NIST. (2022). Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology.
17. UNCTAD. (2024). Digital Economy Report 2024. United Nations.
18. World Bank. (2023). World Development Indicators & Governance Indicators. Washington, DC.
19. World Bank. (2023). Digital Economy Projects and Regulatory Sandboxes Report.
20. World Economic Forum. (2024). Global Cybersecurity Outlook 2024.
21. ITU. (2024). Global Cybersecurity Index 2024. International Telecommunication Union.
22. Rosseel, Y. (2012). lavaan: An R package for structural equation modeling. Journal of Statistical Software, 48(2), 1–36.
23. Rodrik, D. (2004). Industrial policy for the twenty-first century. Harvard University.