# ESSENTIAL CONDITIONS FOR CYBERSECURITY IN ECONOMIC PROGRESS

**Valiyev B B**
*University of Public Safety of Republic of Uzbekistan*
*professor of the Department of Economic Sciences*
**Anarkulov A D**
*Deputy Head of the Department*

**Abstract:** *This article provides a comprehensive analysis of the theoretical and practical issues related to ensuring cybersecurity within the digital economy. It emphasizes the strategic, institutional, legal, and technological reform measures being carried out in Uzbekistan in this area. In particular, the study examines the formulation of cybersecurity strategies, the enhancement of public–private sector cooperation, the modernization of information technology infrastructure, and the broadening of international collaboration. Furthermore, drawing on scientific sources, the article discusses global cyberattack statistics, their economic consequences, and the major forms of cyber threats.*

**Keywords:** *digital economy, cybersecurity, cyberattacks, information security, digital transformation, artificial intelligence, blockchain, cryptography, data protection, economic security, IT infrastructure, cyber threats, public policy, international cooperation.*

The analysis of scientific research and existing regulatory and legal sources demonstrates that reforms aimed at strengthening cybersecurity in the republic are being consistently implemented across several interconnected directions, including strategic planning, institutional development, technological modernization, and the expansion of international cooperation. In the context of the rapid development of the digital economy in Uzbekistan, reforms focused on ensuring cybersecurity have, in recent years, acquired a comprehensive and systematic character and are increasingly emerging as one of the most important priority areas of state policy. These transformations are closely linked to the acceleration of digitalization processes in the country, the active introduction of modern information and communication technologies across various sectors of the economy, and the growing number and complexity of cyber threats on a global scale.

First and foremost, particular importance should be attached to the formation of a long-term strategic approach toward ensuring cybersecurity in the country. In particular, based on the Presidential Decree adopted on March 10, 2026, the Cybersecurity Strategy for 2026–2030, along with a corresponding “roadmap” aimed at its practical implementation, was approved. This strategic document encompasses priority tasks such as coordinating the activities of state bodies and organizations in the field of cybersecurity, ensuring the reliable protection of critical information infrastructure, and further improving systems for rapid response to cyberattacks and other digital threats. At the same time, the document defines the conceptual foundations for ensuring national security in the context of the digital economy and serves to strengthen the legal and

organizational mechanisms of reforms in this sphere. As a result, a solid regulatory and legal framework has been established for the consistent implementation of long-term state policy aimed at developing cybersecurity in the country.

In addition, significant attention is being devoted to the implementation of institutional reforms in the field of cybersecurity. In particular, specialized divisions responsible for information and cybersecurity issues are being established within public administration bodies, and their powers are being gradually expanded. Alongside this, practical measures are being undertaken to improve the activities of specially authorized institutions, strengthen the capabilities of national computer incident response centers, and enhance their technical capacity. This contributes to the establishment of cybersecurity as a distinct strategic direction within the system of public administration and increases its overall effectiveness. Furthermore, strengthening cooperation between the public and private sectors in ensuring cybersecurity is recognized in Uzbekistan as one of the priority tasks. In particular, initiatives aimed at forming and further developing the national cybersecurity ecosystem are consistently expanding through the support of information technology companies, innovation centers, and technological startups operating in the digital sphere. These processes contribute not only to the creation and implementation of advanced digital technologies, but also to improving the professional capacity of local specialists, strengthening the security of digital services, and ensuring the uninterrupted and stable functioning of information systems used across various sectors of the economy. In this way, a comprehensive cybersecurity system aimed at ensuring the secure, stable, and reliable development of the digital economy is being gradually formed in the country.

Within this process, the activities of IT Park Uzbekistan hold particular strategic significance. This technology park is making a substantial contribution to strengthening the national cybersecurity infrastructure by supporting the development of the IT industry, promoting innovative projects, and training highly qualified specialists. In particular, through modern educational programs, startup acceleration projects, international cooperation platforms, and practical training sessions organized within the framework of IT Park, specialists operating in the field of cybersecurity are being trained. At the same time, a number of initiatives are being implemented to introduce advanced foreign experience, apply innovative technologies in practice, and develop the digital skills of young people. This, in turn, is becoming one of the key factors in ensuring cybersecurity through the development of human capital and the enhancement of the potential of personnel possessing modern knowledge and skills.

Another important direction of the cybersecurity reforms being carried out in Uzbekistan is connected with improving the regulatory and legal framework in accordance with modern requirements. The rapid development of digital technologies and artificial intelligence systems necessitates the creation of new legal mechanisms. In this regard, legislative initiatives aimed at regulating the use of artificial intelligence technologies and protecting personal data are being developed in the country. In particular, the drafting of a law in 2025 aimed at legally regulating the processes of using

artificial intelligence and ensuring the protection of citizens' personal data became one of the significant steps in this direction. This initiative serves to strengthen cybersecurity from a legal perspective, ensure data security on digital platforms, and protect the interests of users.

Moreover, these legislative initiatives are aimed at preventing risks associated with the unlawful collection, processing, storage, and dissemination of information, ensuring openness and transparency in the use of digital services, and protecting users' rights and interests related to information security. At the same time, extensive measures are being implemented to introduce ethical principles in the use of artificial intelligence technologies, develop mechanisms that comply with international security standards, and establish modern, reliable, and protected systems for handling data within the activities of state bodies and the private sector. As a result, the modern legal, organizational, and institutional foundations for ensuring cybersecurity in the context of the digital economy are being gradually strengthened in Uzbekistan, thereby contributing to the protection of the national information space.

The development of technological infrastructure is also considered one of the priority directions in ensuring cybersecurity. In recent years, large-scale projects have been implemented in the country to modernize digital infrastructure, establish modern data centers, widely introduce cloud technologies, and integrate various information systems. On the one hand, these processes ensure the uninterrupted and efficient functioning of the digital economy, while on the other hand, they contribute to strengthening the security of information resources and digital platforms. In particular, the introduction of modern protection mechanisms in public administration, the banking and financial sector, the energy industry, telecommunications, and electronic services serves as an important factor in enhancing the level of cybersecurity. At the same time, due to the growing demand for cybersecurity services and technologies in the country, this market is also developing rapidly. According to analytical assessments, the cybersecurity market demonstrates annual growth rates averaging between 25 and 30 percent. This indicates that the sector is becoming not only strategically important from the perspective of security, but also from the standpoint of economic development, attracting investments, and promoting innovative technologies. Consequently, cybersecurity is gradually emerging as a separate and promising branch of the economy.

The relevance of the cybersecurity reforms being implemented in Uzbekistan is also explained by the sharp increase in the number of cyber threats and cybercrimes in the country. According to statistical data, the number of cybercrimes increased several times during the period from 2021 to 2025, highlighting the need to pay serious attention to security issues within the digital environment. Furthermore, in 2024 alone, tens of thousands of cyber threats and hundreds of cybersecurity-related incidents were recorded. In particular, the banking and financial system, the energy sector, and the field of information and communication technologies have increasingly become the primary targets of cyberattacks. These circumstances demonstrate the necessity of further

accelerating reforms aimed at strengthening cybersecurity in order to ensure the stable functioning of the digital economy.

In addition, the development of international cooperation in the field of cybersecurity is regarded in Uzbekistan as one of the key strategic directions for ensuring digital security. In particular, international forums and conferences such as the "Cybersecurity Summit – Central Eurasia, CSS 2025," organized in the city of Tashkent, serve as important platforms for the exchange of regional and global experience, the study and implementation of advanced technologies, and the strengthening of international cooperation ties. Through such events, cooperation with foreign experts, international organizations, and technology companies is expanding, while Uzbekistan's integration into the global cybersecurity system is becoming increasingly strengthened. This, in turn, serves as an important factor in enhancing the country's digital security potential in the international arena.

Overall, the reforms being implemented in Uzbekistan to ensure cybersecurity in the context of the digital economy possess a comprehensive and systematic character, encompassing such important areas as strategic planning, institutional development, improvement of the regulatory and legal framework, the formation of modern technological infrastructure, and the expansion of international cooperation. As a result of these reforms, it can be observed that the level of cybersecurity in the country is gradually increasing and that the necessary organizational, technological, and legal conditions for the secure and sustainable development of the digital economy are being established.

In recent years, the issue of ensuring cybersecurity in the context of the digital economy has come to be viewed not merely as a technical or software-related problem, but rather as an important component of a broad socio-economic, institutional, and global security system. Modern scientific research and theoretical approaches demonstrate that the acceleration of digitalization processes has encompassed nearly all sectors of economic activity, leading to the formation of a new economic model — the digital economy. Within this model, data emerge as one of the most important strategic resources, and their integrity, reliability, and security are becoming fundamental factors in ensuring economic stability and national competitiveness. For this reason, the issue of cybersecurity has become one of the priority areas of modern scientific research, with particular attention being devoted to the in-depth study of its economic, technological, legal, and institutional dimensions. In particular, the development of digital platforms, electronic commerce, artificial intelligence, cloud technologies, and systems for processing large volumes of data necessitates the creation of new approaches and innovative protection mechanisms for ensuring cybersecurity. Consequently, cybersecurity is acquiring strategic significance as an integral component of the modern digital economy and is occupying an important place in the long-term development policies of states and organizations.

According to contemporary scientific perspectives, the formation and rapid development of the digital economy are inseparably connected with the extensive

application of information and communication technologies across all sectors of the economy. Although the deepening of digitalization processes increases efficiency in production, finance, trade, services, and management systems, it simultaneously gives rise to new forms of risks and threats. In particular, the scientific study entitled “Digital Economy: Trends, Challenges, and Development Prospects” emphasizes that digital technologies have become the primary driving force of modern economic development. The authors of the study note that digital platforms, artificial intelligence, big data, and cloud technologies significantly enhance the efficiency of economic activities, while also highlighting that the risks associated with these processes are increasing. In particular, it is substantiated that cybersecurity-related threats are generating complex and multidimensional problems for states, business entities, and society as a whole.

This scientific research provides a profound analysis of the development trends of the digital economy and particularly emphasizes the necessity of establishing effective security mechanisms to ensure its sustainable development. According to the authors, the increasing digitalization of economic systems is transforming data into a strategic resource. As a result, ensuring data security, creating effective protection systems against cyberattacks, and maintaining the stable functioning of information infrastructures are emerging as important prerequisites for the uninterrupted development of the digital economy. Therefore, cybersecurity is interpreted not only as a technological issue, but also as a field of significant economic and strategic importance.

In scientific works published in recent years, cybersecurity is increasingly interpreted as an integral component of economic security. In particular, the article entitled “Economic Security in the Digital Economy” identifies cyberattacks, violations of data confidentiality, illegal information exchange, and issues related to the regulation of digital activities as the main threats arising from digital transformation processes. The study scientifically substantiates that these threats directly affect the stability and efficient functioning of economic systems. In particular, it is emphasized that the increasing dependence of financial systems, e-commerce platforms, public administration, and strategic infrastructures on digital technologies is making them more vulnerable to cyber risks.

The author of this article advances the idea that, in order to reduce cybersecurity-related threats and ensure the stability of economic systems, it is necessary to strengthen cooperation among state bodies, business entities, and civil society institutions. This approach demonstrates that ensuring cybersecurity cannot be limited solely to technical tools or software protection systems, but must also be supported through institutional governance, regulatory and legal mechanisms, and effective state policy. As a result, the issue of cybersecurity is considered a comprehensive management system in which the interaction and harmony of technological, economic, and organizational factors acquire crucial importance.

Other scientific approaches emphasize that the very essence of the economic security system is fundamentally changing under the conditions of the digital economy,

with cybersecurity occupying a central position within this transformation. In particular, the study entitled “System of Economic Security in the Conditions of the Digital Economy” notes that the large-scale digitalization of the economy is making financial operations, investment processes, electronic payment systems, and critical infrastructures increasingly vulnerable to cyber threats. The authors of the study substantiate that, as information resources and digital platforms acquire strategic significance within modern economic systems, the issue of their protection is becoming a priority direction of national economic security.

From this perspective, the authors particularly emphasize the necessity of utilizing blockchain technologies, protecting critical infrastructures through multi-layered security systems, safeguarding data through cryptographic methods, and developing comprehensive cybersecurity strategies. In particular, the capabilities of blockchain technology in ensuring data reliability and transparency, the role of artificial intelligence-based security systems in the early detection of threats, and the effectiveness of automated monitoring systems are evaluated as important factors in ensuring modern economic security. This demonstrates that innovative technologies are increasingly becoming not only instruments of economic development, but also strategic tools for ensuring security.

In general, the analysis of modern scientific literature demonstrates that the issue of cybersecurity in the context of the digital economy is closely interconnected with economic security, institutional governance, and technological progress. As digitalization processes deepen and data and information systems transform into strategic resources, the issue of their protection is becoming one of the priority directions for states, business entities, and international organizations. Therefore, ensuring cybersecurity is gaining increasing scientific and practical relevance as one of the key factors guaranteeing the stability, competitiveness, and continuous development of modern economic systems.

Security issues also occupy a special place in studies devoted to examining the stages of formation and development of the digital economy. The article entitled “Digital Economy: Essence, Features and Stages of Development” identifies automation, computerization, and reliance on information technologies as the main characteristics of the digital economy, while emphasizing that these processes give rise to new security requirements. This, in turn, makes it possible to consider cybersecurity as a fundamental element of the digital economy. .

Studies conducted using the example of Uzbekistan also confirm the close interconnection between the digital economy and cybersecurity. In particular, the article entitled “Digital Economy Development in Uzbekistan” notes that while the development of the digital economy contributes to improving the investment climate, financial stability, and transparency, it simultaneously increases the necessity of ensuring data security. . Furthermore, the study entitled “Prospects for Developing the Country's Economy Through Digital Investments in Uzbekistan” emphasizes that while investments in digital infrastructure stimulate economic growth, it is also necessary to define

cybersecurity as a strategic priority area. In these scientific works, cybersecurity is regarded as an integral component of national economic policy.

Recent scientific studies also extensively highlight the role of advanced technologies in ensuring cybersecurity. In particular, artificial intelligence-based threat detection systems, machine learning algorithms, and automated monitoring tools are recognized as effective instruments for ensuring cybersecurity. The study entitled “Securing the Digital World: Protecting Smart Infrastructures and Digital Industries with AI-Enabled Malware and Intrusion Detection” substantiates that modern cyberattacks are becoming increasingly sophisticated and that artificial intelligence-based solutions are of great importance in combating them. This approach makes it possible to automate cybersecurity systems and enhance their overall effectiveness.

In addition, certain scientific sources particularly emphasize the role of the human factor in ensuring cybersecurity alongside the importance of the digital economy in socio-economic development. In other words, users’ digital literacy, security culture, and personnel training issues are considered among the essential components of the cybersecurity system. This aspect is especially relevant for developing countries and is regarded as one of the key factors determining the effectiveness of the digital transformation process. Furthermore, blockchain technologies are also viewed as one of the promising directions for ensuring cybersecurity. The study entitled “A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry” scientifically substantiates that blockchain technologies can enhance the level of cybersecurity by ensuring the integrity, transparency, and immutability of data. This is of significant importance in addressing issues of trust within the digital economy.

Modern research in the field of cryptography also plays an important role in developing the theoretical foundations of cybersecurity. In particular, scientific studies related to quantum cryptography and digital signature technologies are opening new opportunities for ensuring the confidentiality, integrity, and authentication of data. Research conducted in this area considers cryptographic mechanisms as one of the core components of cybersecurity, while improving their effectiveness is recognized as an urgent scientific challenge. Statistical analyses of cyberattacks in recent years indicate that the number and complexity of cyber threats are steadily increasing on a global scale. According to data from Cybersecurity Ventures, by 2025 cybercrime is expected to cause approximately 10.5 trillion US dollars in annual damages to the global economy, making it one of the largest economic threats in human history. At the same time, reports by Check Point Research note that during 2024, each organization faced an average of more than 1,200 cyberattacks per week, indicating an extremely high intensity of attacks.

In cases related to data breaches, analyses by IBM Security show that the average cost of a single incident is around 4.5 million US dollars. When examined by attack type, phishing still remains the most widespread method, accounting for nearly half of all cyberattacks; according to data from Anti-Phishing Working Group, more than one million phishing sites were detected each month in 2024. At the same time, ransomware attacks are also growing rapidly: according to reports by Sophos, approximately 66

percent of companies encountered such attacks, while the average ransom payment approached 1.5 million US dollars.

DDoS attacks have also increased significantly. According to data from Cloudflare, their number has risen by 20–30%, and in some cases, traffic loads reaching terabit levels have been recorded. From a sectoral perspective, the most frequently targeted industries include the financial and banking system, healthcare, education, and government institutions. In particular, the healthcare sector is considered a high-risk group, as the data it handles is highly valuable, while its security systems are often insufficiently developed. From an economic perspective, cyberattacks are affecting not only large companies but also small and medium-sized businesses: according to analyses, a significant proportion of small businesses that fall victim to such attacks are forced to cease operations within six months. It is also noted that approximately 80% of data breach incidents are associated with the human factor—weak passwords, falling victim to phishing, or incorrect configurations. Overall, cyber risks have become an integral challenge of the modern digital economy, requiring a comprehensive approach and continuous monitoring.

In conclusion, the analysis of scientific literature published over the past five years interprets cybersecurity as an integral and strategically important element of the digital economy. Based on these studies, the theoretical foundations of cybersecurity are developing along the following conceptual directions: first, cybersecurity is considered an integral part of the economic security system; second, state policy and institutional mechanisms play a crucial role in ensuring it; third, innovative technologies such as artificial intelligence, blockchain, and cryptography are emerging as key tools; and fourth, the concept of risk management and a comprehensive approach is recognized as a priority methodological framework. Therefore, ensuring cybersecurity in the context of the digital economy is emerging as a complex scientific and practical issue that requires a multi-level, systematic, and integrated approach.

In Uzbekistan, further improvement of reforms aimed at ensuring cybersecurity in economic development is considered one of the key factors for the sustainable development of the modern digital economy. First of all, it is necessary to continuously improve the national cybersecurity strategy in line with modern requirements. In this process, strengthening cooperation between state bodies, the private sector, and civil society institutions, as well as clearly defining their roles and responsibilities, is of great importance. In particular, it is essential to strengthen information security in strategic sectors such as banking and finance, energy, transport, telecommunications, and healthcare, equip critical infrastructures with modern protection systems, and regularly conduct security audits. At the same time, human capital development should be one of the priority directions in ensuring cybersecurity. Therefore, it is advisable to expand educational programs in cybersecurity and information security at higher education institutions, establish practical laboratories, and introduce qualification improvement systems aligned with international standards. In addition, training young people in programming, artificial intelligence, and information security from an early stage will

help form a pool of qualified specialists. This, in turn, will contribute to improving the effectiveness of the national cybersecurity system in the future.

Developing cooperation between the public and private sectors is also an important factor in ensuring cybersecurity. Establishing mechanisms for information sharing and rapid response to threats between IT companies, banks, telecommunications operators, and government institutions plays a crucial role in reducing cyber risks. At the same time, supporting startups and innovative projects, developing the national cybersecurity ecosystem, and focusing on the creation of local software products and protection systems are essential. This will help reduce dependence on foreign technologies and strengthen national digital independence. In the context of the digital economy, the effective use of artificial intelligence, blockchain, and big data processing technologies is also highly important for ensuring cybersecurity. In particular, the introduction of AI-based monitoring systems can enhance the ability to detect cyberattacks in advance, automatically analyze risks, and respond promptly. The use of blockchain technologies contributes to ensuring data security and transparency.

Furthermore, it is necessary to improve the regulatory and legal framework in accordance with international standards. In particular, further development of legislation regulating personal data protection, electronic commerce, artificial intelligence, and digital service security is essential. At the same time, increasing users' legal awareness of information security, promoting safe internet usage culture, and strengthening awareness campaigns on cybersecurity are also urgent tasks, as many cyberattacks occur due to the human factor and insufficient user knowledge. In addition, it is advisable to further strengthen the activities of national cyber incident response centers, expand their technical and organizational capabilities, and introduce modern monitoring systems. Developing mechanisms for real-time threat detection and response will help strengthen the security of digital infrastructures. Moreover, expanding cooperation with international organizations and foreign countries, sharing experience, and implementing joint projects will enhance Uzbekistan's integration into the global cybersecurity system. Overall, ensuring cybersecurity in the economic development of Uzbekistan requires the coordinated implementation of strategic planning, modern technologies, skilled workforce training, improvement of the regulatory and legal framework, and development of international cooperation. These factors collectively serve as one of the main conditions for ensuring the secure, stable, and efficient development of the digital economy.

## REFERENCES:

1. Law of the Republic of Uzbekistan "On Electronic Government"
2. Law of the Republic of Uzbekistan "On Electronic Commerce"
3. United Nations (UN) – Cybersecurity Resources
4. International Telecommunication Union (ITU) – Global Cybersecurity Index
5. World Economic Forum – Cybersecurity Reports

6. Kaspersky Cybersecurity Resource Center
7. Cisco Cybersecurity Reports and Insights
8. ISO/IEC 27001 Information Security Management Standards
9. Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson Education, 2020.
10. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.
11. Schneier, B. Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley, 2015.
12. Laudon, K. C., Laudon, J. P. Management Information Systems: Managing the Digital Firm. Pearson, 2022.
13. Turdiev, J., Axmedov, B. “Issues of Ensuring Cybersecurity in the Context of the Digital Economy.” Journal of Economics and Innovative Technologies, 2023. Abduqodirov, A. “O‘zbekistonda axborot xavfsizligi tizimini rivojlantirish istiqbollari.” Axborot xavfsizligi muammolari jurnali, 2022.