

JOURNAL OF DIGITAL LAW AND INNOVATION (JDLI)

LAW • TECHNOLOGY • INNOVATION • JUSTICE

 OPEN
ACCESS

INTERNATIONAL
PEER-REVIEWED
JOURNAL



OUR FIELDS

- Digital law
- Cybersecurity law
- Artificial intelligence and robotics law
- Intellectual property law
- LegalTech and legal innovations
- E-government and digital public services
- Legal aspects of AgroTech and GreenTech
- Smart city and digital governance



OUR INDEXING



Google Scholar

zenodo Zenodo



DOI



OpenAIRE



Open Access



DIGITAL LAW



<https://unireview.uz/index.php/jdli>



Published by
UniLex Global, Uzbekistan



VOLUME 1

ISSUE 1



JUNE 2026



“UNILEX GLOBAL” LLC

**Raqamli huquq va innovatsiya
jurnali**

**Journal of Digital Law and
Innovation**

June, 2026

VOLUME 1, ISSUE 1



EDITORIAL TEAM

Editor-in-Chief, Tukhtashev Hikmatilla Ismatillaevich - Head of the Department of Legal Sciences, Doctor of Philosophy in Legal Sciences (PhD), TIAME National Research University, Tashkent, Republic of Uzbekistan.

1. **Editorial Board Member Borotov Mirodiljon Xomudjonovich** — Doctor of Legal Sciences, Professor, Head of the Department of Civil Law, International Law and International Organizations, Institute of State and Law of the Academy of Sciences of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
2. **Editorial Board Member Maripova Sevarxon Aribjanovna** — Doctor of Philosophy in Legal Sciences (PhD), Associate Professor, Department of Social Sciences, Cyber University State University, Tashkent, Republic of Uzbekistan.
3. **Editorial Board Member Kaharova Munira Maxamajanovna** — Doctor of Political Sciences (DSc), Researcher, Institute of Criminology of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
4. **Editorial Board Member Yuldashev Mutalib Ibrohimovich** — Doctor of Economic Sciences, Professor, Department of Economics, Tashkent University of Science and Technology, Tashkent, Republic of Uzbekistan.
5. **Editorial Board Member Bafaev Shukhrat Gafurovich** — Doctor of Legal Sciences, Head of the Tashkent City Branch, Center for the Analysis of Democratic Processes, Tashkent, Republic of Uzbekistan.
6. **Editorial Board Member Khodjaeva Aziza Bakhtiyarovna** — Doctor of Philosophy in Legal Sciences (PhD), “Academy of Labor and Social Relations” under the Federation of Trade Unions of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
7. **Editorial Board Member Khudoyberdieva Viloyat Jabbrovanovna** — Candidate of Legal Sciences (PhD), Olmazor District Department of Public Education, Tashkent City, Republic of Uzbekistan.
8. **Editorial Board Member Boboumarova Munira Kurbonovna** — Doctor of Philosophy in Legal Sciences (PhD), Department for Organization of Investigative Activities, Investigation Division, Tashkent City Internal Affairs Department, Tashkent, Republic of Uzbekistan.
9. **Editorial Board Member Usmonov Vosid Muhammadievich** — Doctor of Philosophy in Legal Sciences (PhD), Diplomatic University, Tashkent, Republic of Uzbekistan.
10. **Editorial Board Member Mirzayeva Malika Baxadirovna** — Doctoral Researcher, PhD, Associate Professor, Department of Digital Technologies and Artificial Intelligence, Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
11. **Editorial Board Member Allayorov Tulqin Ruziqulovich** — Doctor of Philosophy in Philology (PhD), Associate Professor, Nizami Named Tashkent State Pedagogical University, Tashkent, Republic of Uzbekistan.
12. **Editorial Board Member Tosheva Maftuna Anvar kizi** — Doctor of Philosophy in Legal Sciences (PhD), Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
13. **Editorial Board Member Askarov Jaloliddin Toychievich** — Doctor of Philosophy in Legal Sciences (PhD), Deputy Head, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
14. **Editorial Board Member Abdixakimov Islombek Bahodir o'g'li** — Master of Law (LL.M), Head of the Artificial Intelligence and Legal Tech Laboratory, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
15. **Editorial Board Member Kalandarov Aminjon Amondullayevich** — Doctor of Philosophy in Legal Sciences (PhD), Acting Associate Professor, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
16. **Editorial Board Member Hakimov Komil Bakhtiyarovich** — Doctor of Legal Sciences (DSc), Professor, Head of the Department of Criminal Law, Criminology and Anti-Corruption, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.

CONTENTS

03

**XUDOYBERDIYEV XUMOYUNBEK XABIBULLA O'G'LI,
QURVONBOYEV ASLBEK AZIZJON O'G'LI**

KIBERXAVFSIZLIKNING KONSTITUTSIYAVIY ASOSLARI
VA MILLIY XAVFSIZLIKKA TA'SIRI

13

SATTAROV ULUG'BEK UMED O'G'LI

RAQAMLI IQTISODIYOT SHAROITIDA KIBERXAVFSIZLIK
MUAMMOLARI: ZAMONAVIY XAVFLAR VA BARQAROR
RIVOJLANISH YONDASHUVLARI

20

MANNABJONOVA DURDONA ABDUXALIL QIZI

DAVLAT IDORALARIDA SUN'IY INTELLEKTDAN
FOYDALANISHNI HUQUQIY TARTIBGA SOLISH

34

HUSANOVA SHABBONA BAHROMOVNA

RAQAMLI MUHITDA INTELLEKTUAL MULK
HUQUQINING MUHOFAZASI

40

RIXSIYEV MUHAMMADAZIZ MUZAFFAR O'G'LI

O'ZBEKISTON RESPUBLIKASIDA
KIBERJINOYATCHILIKKA QARSHI KURASHISHNING
KONSITUTSIYAVIY-HUQUQIY VA XALQARO-
HUQUQIY ASOSLARI

54

BOYMIRZAYEVA MADINA IBROHIM QIZI

SUN'IY INTELLEKTNING HUQUQ TIZIMLARI VA ODIL
SUDLOV FAOLIYATIGA TA'SIRI



RAQAMLI IQTISODIYOT SHAROITIDA KIBERXAVFSIZLIK MUAMMOLARI: ZAMONAVIY XAVFLAR VA BARQAROR RIVOJLANISH YONDASHUVLARI

Sattarov Ulug'bek Umed o'g'li

“TIQXMMI” Milliy tadqiqot universiteti, “Iqtisodiyot” fakulteti “Buxgalteriya hisobi” ta’lim yo’nalishi 2-kurs talabasi

MAQOLA MA'LUMOTI

Kalit so'zlar:

raqamli iqtisodiyot,
kiberxavfsizlik,
kiberxavflar,
ma'lumotlarni himoya qilish,
raqamli transformatsiya,
axborot tizimlari,
raqamli infratuzilma,
sun'iy intellekt, blokcheyn,
iqtisodiy xavfsizlik.

ANNOTATSIYA

Ushbu maqolada raqamli iqtisodiyotda kiberxavfsizlikni ta'minlashning nazariy asoslari va amaliy muammolari tahlil qilinadi. Raqamli transformatsiya (sun'iy intellekt, blokcheyn, bulutli texnologiyalar) iqtisodiy o'sishni rag'batlantirish bilan bir qatorda, murakkab kiberxavflar, ma'lumotlar sizib chiqishi va to'lov dasturlari (ransomware) bilan bog'liq tahdidlarni ham yuzaga keltirmoqda. Tadqiqot xalqaro boshqaruv va normativ-huquqiy bazalarni o'rganib, infratuzilmasi hamda tajribasi cheklangan rivojlanayotgan davlatlarning zaif jihatlarini ochib beradi. Yakuniy xulosalar kiberxavfsizlikni mustahkamlash barqaror iqtisodiy o'sish va uzoq muddatli barqarorlikning fundamental sharti ekanligini ko'rsatadi.

CYBERSECURITY CHALLENGES IN THE DIGITAL ECONOMY: MODERN RISKS AND SUSTAINABLE DEVELOPMENT APPROACHES

ARTICLE INFO

Keywords:

digital economy,
cybersecurity,
cyber threats, data protection,
digital transformation,
information systems, digital
infrastructure, artificial
intelligence, blockchain,
economic security

ABSTRACT

This article analyzes the theoretical foundations and practical challenges of cybersecurity in the digital economy. While digital transformation (AI, blockchain, cloud computing) drives economic growth, it simultaneously escalates exposure to complex cyber threats, data breaches, and ransomware. Examining international governance and regulatory frameworks, the study highlights the vulnerabilities of developing economies due to limited infrastructure and expertise. The findings conclude that strengthening cybersecurity is a fundamental requirement for sustainable economic growth and long-term resilience

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ: СОВРЕМЕННЫЕ РИСКИ И ПОДХОДЫ УСТОЙЧИВОГО РАЗВИТИЯ

ИНФОРМАЦИЯ СТАТЬИ

Ключевые слова:

цифровая экономика,
кибербезопасность,
киберугрозы,
защита данных,
цифровая трансформация,
информационные системы,
цифровая инфраструктура,
искусственный интеллект,
блокчейн, экономическая
безопасность.

АННОТАЦИЯ

В данной статье анализируются теоретические основы и практические проблемы обеспечения кибербезопасности в цифровой экономике. В то время как цифровая трансформация (искусственный интеллект, блокчейн, облачные вычисления) стимулирует экономический рост, она одновременно увеличивает уязвимость перед комплексными киберугрозами, утечками данных и программами-вымогателями. Исследуя международные подходы к управлению и нормативно-правовую базу, авторы выделяют уязвимости развивающихся стран, обусловленные ограниченной инфраструктурой и нехваткой опыта. Результаты исследования подтверждают, что укрепление систем кибербезопасности является фундаментальным условием для устойчивого экономического роста и долгосрочной стабильности.

INTRODUCTION

The development of the digital economy represents one of the most significant transformations in modern global economic systems. Over the past two decades, traditional economic structures have gradually shifted toward digital platforms where goods, services, and financial transactions are conducted electronically. This transformation has been driven by rapid technological advancements in information and communication technologies, including internet expansion, mobile technologies, cloud computing, and artificial intelligence systems [1].

The digital economy has significantly improved productivity, reduced transaction costs, and increased access to global markets. Businesses are now able to operate across borders with minimal physical infrastructure, while consumers benefit from faster and more efficient services. Governments have also adopted digital technologies to improve public service delivery through e-government systems and digital identification platforms.

However, alongside these advantages, the digital transformation process has introduced new risks that were not present in traditional economic systems. The increasing reliance on interconnected digital networks has created new vulnerabilities that can be exploited by cybercriminals. As a result, cybersecurity has become a fundamental requirement for ensuring the stability and sustainability of modern economies.

Cybersecurity refers to the protection of computer systems, networks, programs, and data from unauthorized access, attacks, damage, or disruption. It is no longer limited to technical protection but has evolved into a strategic component of national economic security and global stability [2].

In recent years, cyberattacks have become more sophisticated, organized, and financially motivated. Criminal groups and even state-sponsored actors are increasingly targeting critical infrastructure, financial systems, healthcare institutions, and government databases. These attacks can lead to severe financial losses, disruption of essential services, and loss of public trust in digital systems.

The importance of cybersecurity is particularly high in the context of the digital economy, where data is considered one of the most valuable economic assets. The loss or manipulation of data can have significant consequences for businesses and governments, affecting decision-making processes, operational efficiency, and strategic planning.

In developing countries, including Uzbekistan, the digital transformation process is progressing rapidly. The introduction of e-government services, digital banking systems, and electronic payment platforms has significantly improved economic efficiency and accessibility. However, the rapid expansion of digital infrastructure without sufficient cybersecurity readiness increases exposure to cyber threats [3].

Therefore, analyzing cybersecurity challenges in the digital economy is essential for developing effective protection strategies and ensuring sustainable economic development.

METHODOLOGY

The research methodology of this study is based on a systematic and comparative approach aimed at analyzing cybersecurity challenges within the digital economy framework. The study combines qualitative analysis, comparative international review, and interpretation of statistical data from global cybersecurity reports.

Firstly, the theoretical foundation of the digital economy and cybersecurity was examined through academic literature, policy documents, and international reports published by organizations such as the World Bank, International Telecommunication Union (ITU), and the Organization for Economic Cooperation and Development (OECD) [4]. These sources provided a comprehensive understanding of global cybersecurity trends and digital transformation dynamics.

Secondly, a comparative analysis was conducted between developed and developing countries to evaluate differences in cybersecurity maturity levels. Countries such as the United States, Germany, South Korea, Japan, and Singapore were used as benchmarks for advanced cybersecurity systems. Their approaches were compared with those of emerging economies to identify structural weaknesses and institutional gaps.

Thirdly, national strategies and regulatory frameworks were analyzed, with particular focus on digital transformation policies and cybersecurity development programs. This included examining legal frameworks, institutional responsibilities, and national cybersecurity strategies.

The study also utilized key analytical indicators, including the frequency of cyber incidents, financial losses caused by cybercrime, investment levels in cybersecurity infrastructure, and human capital development in the cybersecurity sector. These indicators were used to evaluate the effectiveness of cybersecurity systems in different economic environments.

ANALYSIS AND RESULTS

The digital economy is fundamentally based on the integration of digital technologies into all aspects of economic activity. While this integration provides significant benefits in terms of efficiency, innovation, and accessibility, it also creates new security vulnerabilities.

One of the most significant challenges in the digital economy is the increasing number of cyberattacks targeting both public and private sector organizations. Cybercriminals use a wide range of techniques, including malware, phishing, ransomware, spyware, and distributed denial-of-service (DDoS) attacks, to compromise digital systems.

Financial institutions are among the most frequently targeted sectors due to the high value of financial data and transactions. Online banking systems, digital wallets, and electronic payment platforms are particularly vulnerable to cyber fraud and data breaches. According to international cybersecurity reports, the financial sector experiences billions of dollars in losses annually due to cybercrime [5].

Another critical issue is data security. In the digital economy, data has become a central economic resource. Businesses rely on data analytics to make strategic decisions, optimize operations, and understand consumer behavior. However, unauthorized access to sensitive data can lead to severe consequences, including financial loss, reputational damage, and legal penalties.

Cloud computing technologies have further increased the complexity of cybersecurity. While cloud systems provide scalability and cost efficiency, they also introduce risks related to data storage, access control, and third-party service providers. Ensuring the security of cloud-based systems requires advanced encryption methods and strict access management policies.

Artificial intelligence (AI) has also transformed the cybersecurity landscape. AI-based systems are increasingly used to detect anomalies, identify threats, and respond to cyberattacks in real time. However, cybercriminals are also using AI technologies to develop more sophisticated attack methods, creating an ongoing technological competition between attackers and defenders.

Another important dimension of cybersecurity in the digital economy is the increasing interconnection of critical infrastructure systems. Energy networks, transportation systems, healthcare services, and communication infrastructures are now heavily dependent on digital technologies. While this integration improves efficiency and service delivery, it also creates systemic risks where a single cyberattack can disrupt entire economic and social systems [6]. For example, attacks on energy grids or transportation control systems can lead to large-scale disruptions affecting not only individual organizations but also national economic stability. This phenomenon demonstrates that cybersecurity is no longer limited to protecting individual users or companies; it has become a matter of national security and economic resilience.

Ransomware attacks have become one of the most damaging forms of cybercrime in recent years. In such attacks, malicious software encrypts an organization's data and demands payment for its release. These attacks have targeted hospitals, financial institutions, universities, and government agencies, causing significant operational disruptions. The economic impact of ransomware is increasing annually, with global losses reaching billions of dollars [7].

Phishing attacks also remain a major threat in the digital economy. Cybercriminals use deceptive emails, messages, or websites to trick users into revealing sensitive information such as passwords, bank details, and personal identification data. Despite technological advancements, human error remains one of the weakest links in cybersecurity systems.

Social engineering attacks exploit psychological manipulation rather than technical vulnerabilities. These attacks highlight the importance of human factors in cybersecurity. Even the most advanced technological systems can be compromised if users lack awareness or training in identifying cyber threats.

Another important challenge is the shortage of cybersecurity professionals. The rapid growth of digital technologies has created a high demand for skilled experts in information security, ethical hacking, and network protection. However, many countries face a significant gap between demand and supply of qualified cybersecurity specialists. This shortage weakens the overall resilience of digital systems [8].

Investment in cybersecurity infrastructure is also uneven across countries. Developed economies allocate significant resources to cybersecurity research, advanced monitoring systems, and threat intelligence platforms. In contrast, developing countries often struggle with limited budgets, outdated systems, and insufficient institutional capacity.

DISCUSSION

The findings of this study indicate that cybersecurity is a fundamental pillar of the digital economy. Without effective cybersecurity systems, digital transformation efforts may lead to increased vulnerability rather than sustainable economic growth.

One of the key issues identified is the rapid evolution of cyber threats. Cybercriminals continuously develop new methods to bypass security systems, making it difficult for organizations to maintain long-term protection. This requires constant updates to cybersecurity technologies and policies.

Another major issue is the imbalance between technological development and regulatory frameworks. In many cases, digital technologies evolve faster than legal and institutional systems. As a result, governments struggle to regulate emerging cyber risks effectively. This regulatory gap creates opportunities for cybercriminal activities.

International cooperation plays a crucial role in addressing cybersecurity challenges. Since cyber threats often cross national borders, no single country can effectively combat cybercrime alone. Global collaboration in intelligence sharing, legal enforcement, and technological development is essential for building a secure digital environment [9].

Public awareness is also a critical factor. Many cyber incidents occur due to lack of knowledge among users regarding safe digital practices. Therefore, improving digital literacy and cybersecurity awareness among the population is essential for reducing risks associated with human error.

In the context of developing countries, including Uzbekistan, strengthening cybersecurity requires a multi-dimensional approach. This includes investment in modern digital infrastructure, development of specialized education programs, establishment of cybersecurity institutions, and improvement of legal frameworks.

Furthermore, cooperation between public and private sectors is essential. Private companies often possess advanced technological capabilities and expertise, while governments provide regulatory support and national coordination. A strong partnership between these sectors can significantly improve cybersecurity resilience.

CONCLUSION

This study demonstrates that cybersecurity is an essential requirement for the sustainable development of the digital economy. As economic systems become increasingly digitalized, the importance of protecting information systems, digital assets, and communication networks continues to grow.

Cybersecurity challenges are complex and multidimensional, involving technological, organizational, economic, and human factors. Addressing these challenges requires a comprehensive strategy that includes technological innovation, regulatory development, human capital investment, and international cooperation.

The digital economy offers significant opportunities for economic growth, innovation, and efficiency. However, without strong cybersecurity systems, these benefits may be undermined by increasing cyber threats and vulnerabilities.

Therefore, strengthening cybersecurity infrastructure, improving digital literacy, and developing skilled professionals are essential steps toward ensuring long-term economic stability and sustainable development in the digital era.

REFERENCES

1. O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi. “Raqamli O‘zbekiston – 2030 strategiyasi”. <https://mitc.uz/>
2. O‘zbekiston Respublikasi Qonunchilik ma’lumotlari milliy bazasi. “Elektron hukumat to‘g‘risidagi normativ-huquqiy hujjatlar”. <https://lex.uz/>
3. O‘zbekiston Respublikasi Prezidenti. PQ-4699-son qaror: Raqamli iqtisodiyot va elektron hukumatni rivojlantirish chora-tadbirlari (2020). <https://lex.uz/docs/4751561>
4. O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida” Qonuni. <https://lex.uz/docs/2613718>
5. O‘zbekiston Respublikasi Statistika agentligi. Raqamli iqtisodiyot ko‘rsatkichlari bo‘yicha statistik ma’lumotlar (2025). <https://stat.uz/>
6. Elektron hukumat loyihalarini boshqarish markazi. <https://egov.uz/>
7. World Bank. Uzbekistan Digital Development Overview (2023). <https://www.worldbank.org/en/country/uzbekistan>
8. World Economic Forum. Global Cybersecurity Outlook 2024. <https://www.weforum.org/reports/global-cybersecurity-outlook-2024/>
9. International Telecommunication Union (ITU). Global Cybersecurity Index 2024. <https://www.itu.int/>
10. OECD. Digital Economy Outlook 2020. <https://www.oecd.org/digital/>
11. ENISA. Threat Landscape 2023. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
12. NIST. Cybersecurity Framework (CSF) 2.0 (2024). <https://www.nist.gov/cyberframework>
13. IBM Security. Cost of a Data Breach Report 2024. <https://www.ibm.com/reports/data-breach>
14. United Nations Conference on Trade and Development (UNCTAD). Digital Economy Report 2023. <https://unctad.org/publication/digital-economy-report-2023>