

**FOREIGN INVESTMENT AND INFORMATION SECURITY IN THE DIGITAL ECONOMY**

Бабаева Сабинабону Давронбек қизи

Студентка Ташкентского государственного транспортного университета

**ABSTRACT**

In the context of rapid digitalization of the economy, the issues of information security are becoming more and more relevant. The article discusses new approaches to attracting foreign investment, with an emphasis on the risks arising at the same time for strategic digital industries of the Republic of Uzbekistan. The analysis shows that the participation of foreign capital requires a balanced approach and a clear system for protecting the digital sovereignty of the country. steps to improve state policy in the field of information security.

**Keywords:** Digital economy, information security, foreign investment, cybersecurity, digital sovereignty, strategic sectors.

**INTRODUCTION**

The development of the digital economy is significantly transforming the structure of national economies, creating new opportunities and challenges for states. According to international experts, the share of digital components such as data, software and network services is increasing by 7–9% annually in gross value added. This growth indicates that digital technologies are becoming a key driver of economic development. One consequence of this trend is the increase in cross-border data and capital flows, especially in the form of foreign direct investment in information and communication technologies. On the one hand, such investments contribute to technological renewal, infrastructure development and the creation of high-tech jobs. On the other hand, they carry potential risks associated with external influence through control of critical technologies, access to data and digital platforms. These changes require a rethinking of approaches to national security, since if earlier threats were considered mainly in the military or economic plane, today information security is coming to the fore and it covers not only data protection, but also the stability of communication networks, digital systems and critical infrastructure.

This issue is particularly relevant for emerging economies such as the Republic of Uzbekistan. For them, the key task is to find a balance between attracting foreign investment and preserving digital sovereignty. This balance is possible if we develop our own technological competencies, regulate cross-border data and create reliable cybersecurity mechanisms.

Thus, the digital economy is not just technological progress, but a set of socio-economic processes based on the use of data as the main resource, digital communications and platforms. Its development requires a flexible policy that will maximize the benefits and minimize risks in the context of global digital transformation.

Information security is an integral part of national security and includes:

1. Confidentiality and integrity of data.
2. stability of critical information infrastructure.
3. the ability of the state to prevent and counter cyberattacks.
4. sovereign control over the most important digital flows.

From the point of view of institutional theory, the state should create a regulatory environment in which foreign investment does not conflict with the interests of information security.

World experience confirms that in the field of high technology, states are tightening the admission of external capital. The European Union has been applying Regulation No2019/452 since 2020, and the Federal Republic of Germany has reduced the threshold for the acquisition of shares in companies classified as critical infrastructure to 10 percent. Among the key risks:

- Technological control is the ability to install hardware and software vulnerabilities.
- Data leakage is the transfer of sensitive information to foreign jurisdictions.
- Information influence is the use of digital platforms to destabilize the political system.
- Monopoly dependency – critical services (cloud storage, infrastructure as a service, or platform as a service) are controlled by non-residents.

Regulation of foreign direct investment in the digital sphere is becoming a mandatory element of economic policy, which is confirmed by the examples of the United States of America (CHIPS and Science Act of 2022), the People's Republic of China (the Great Firewall of China project) and other countries. Since 2020, the Digital Uzbekistan-2030 strategy has been implemented, which provides for full coverage of the territory with basic telecommunications networks, the development of e-government and the promotion of information technology exports. By the beginning of 2024, the Internet penetration rate reached 83.3 percent, and the number of users exceeded 29.5 million people. Over 675 electronic services are available on the My.gov.uz public services portal, while more than 60 percent of applications are submitted online.

Residents of the Information Technology Park of the Republic of Uzbekistan exported digital services worth \$344 million in 2023 (an increase of 2.4 times compared to 2022). At the same time, the number of non-resident companies reached 426, which confirms the high international interest in the national digital ecosystem. At the same time, there is a concentration of business in the city of Tashkent - about 95 percent of revenue comes from the capital.

In the educational sphere, there is a project "One Million Uzbek Programmers", within the framework of which 1.2 million people were trained in the basics of programming. Specialized schools of cybersecurity and cryptography are being created at the National UNICON.UZ Company and leading higher educational institutions.

Despite significant progress, the number of cyber incidents is growing: in 2024, digital crimes accounted for 44.4 percent of all reported offenses in the country. The main attack methods are malicious links.

To reduce vulnerability in 2024, the Law of the Republic of Uzbekistan "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan in Connection with the Improvement of Legislation in the Field of Cybersecurity" (ZRU No964 of 20.09.2024) was adopted, which expanded the powers of the Central Bank to control information security. The law establishes comprehensive data protection requirements, provides for the revocation of licenses for serious violations, and obliges banks to implement fraud prevention systems.

The Law of the Republic of Uzbekistan dated 02.07.2019 ZRU No547 "On Personal Data" is also in force, which requires the localization of databases on the territory of the Republic of Uzbekistan and toughens responsibility for their loss or unauthorized transfer.

As ways to ensure a safe, stable investment environment, the following measures can be cited: Development of a National Cybersecurity Strategy with a clear delineation of competencies between government agencies, the private sector and civil society. Creation of a foreign direct investment screening system: formation of an interdepartmental committee that evaluates digital projects according to information security criteria. Import substitution of critical technologies: the provision of grants, tax benefits for residents of technology parks and the implementation of public-private partnership mechanisms. Scaling Digital Literacy: Integrating Digital Hygiene into School and University Curricula. annual training of at least 5000 information security specialists. Strengthening international cooperation: participation in the United Nations working groups on cybersecurity, expanding cooperation within the framework of the Shanghai Cooperation Organization and the Commonwealth of Independent States on the exchange of data on cyber threats.

The digital economy opens up opportunities for accelerated development for the Republic of Uzbekistan, but is associated with risks arising in the information space. Attracting foreign investment must be combined with robust safeguards, such as pre-deal analysis, data localization, and regulatory strengthening. The implementation of the proposed measures allows the Republic of Uzbekistan to maintain control over strategically important digital assets, ensuring sustainable and safe development.

## REFERENCES

1. Nadirkhanov U.S. Foreign Investments and Information Security. — Tashkent: TSTU, 2024.
2. Digital transformation of Uzbekistan promotes regional integration in Central Asia // Uzbekistan.org.ua, 2024.
3. Current aspects of digitalization in Uzbekistan // GlobalCIO, 2024.
4. New Cybersecurity Law grants Central Bank enhanced powers to safeguard financial sector // Kun.uz, 21.09.2024.
5. IT Park Uzbekistan summed up its work for 2023 // UzDaily, 31.01.2024.
6. Rising Cybercrime Alarms Uzbekistan's National Security // SpecialEurasia, 03.06.2025.
7. Dentons. Uzbekistan tightens cybersecurity obligations, 14.05.2025.
8. Regulation (EU) 2019/452 establishing a framework for the screening of foreign direct investments.
9. Federal Ministry for Economic Affairs and Energy (Germany). Foreign Trade and Payments Act, amendments 2020.
10. Law of the Republic of Uzbekistan "On Personal Data" (ed. 2021).
11. Strategy "Digital Uzbekistan – 2030" (Presidential Decree No UP-6079, 2020).
12. [https://nrm.uz/contentf?doc=593113\\_&products=1\\_vse\\_zakonodatelstvo\\_uzbekistana](https://nrm.uz/contentf?doc=593113_&products=1_vse_zakonodatelstvo_uzbekistana)
13. [https://naufr.uz/ru/kiberxavfsizlikni\\_taminlash\\_sohasidagi/?ysclid=mcogmsmp8o2480865](https://naufr.uz/ru/kiberxavfsizlikni_taminlash_sohasidagi/?ysclid=mcogmsmp8o2480865)