

INFORMATION AND CYBERSECURITY IN MODERN SOCIETY: LEGAL FRAMEWORKS, THREATS, AND STRATEGIC PROTECTION IN UZBEKISTAN

Boburjon Shokirov

Student of Fergana state university

<https://doi.org/10.5281/zenodo.15474426>

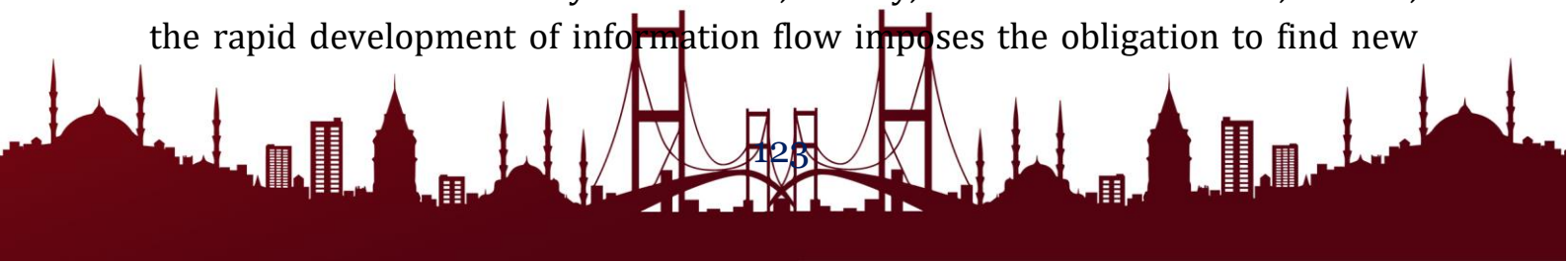
Annotation. In today's global landscape, information security and information-political security have emerged as fundamental pillars for ensuring societal stability, national sovereignty, and international peace. This article explores the growing significance of information and cybersecurity within Uzbekistan, analyzing the legal foundations, technological advancements, and challenges associated with securing data at personal, corporate, and governmental levels. With the increasing frequency of cyberattacks and manipulation of digital information, comprehensive legal regulations such as the Constitution of Uzbekistan and the Law "On Cybersecurity" have been introduced to bolster national protection mechanisms.

Keywords: Information security, Cybersecurity, Personal data protection, Uzbekistan, Information legislation, Digital threats, State Security Service.

Today, information security and information-political security have emerged as critical factors in preserving societal stability and ensuring order both domestically and in the international political arena. Moreover, frequent information attacks visible on the global stage have evolved into a major global issue, necessitating comprehensive scientific and practical investigation into the problems and processes associated with information security.

According to Article 33 of the Constitution of the Republic of Uzbekistan: "Everyone shall have the right to seek, receive and disseminate information. The state shall create the conditions for access to the Internet and global information networks. The right to seek, receive and disseminate information may be restricted only in accordance with the law and only to the extent necessary for the protection of the constitutional order, public health, social morality, the rights and freedoms of others, public security and order, as well as to prevent the disclosure of state secrets or other secrets protected by law" [1].

Information-political security refers to a set of complex issues related to the protection of vital interests of citizens, the state, and society in the political sphere from internal and external information threats. More specifically: first, it aims to ensure the security of the state, society, and citizens' interests; second, the rapid development of information flow imposes the obligation to find new



tools to counter internal and external political threats using information technologies.

Information security has become one of the most pressing issues for individuals, enterprises, and states alike. As the influence of the internet and information technologies continues to grow in our daily lives, so too does the importance of securing information. To understand why we must prioritize information security, consider the following points:

According to Article 4 of the Law of the Republic of Uzbekistan No. O'RQ-547 dated July 2, 2019, "On Personal Data": Personal data refers to information recorded electronically, on paper, or on other tangible media, which pertains to a specific individual or allows for their identification [2].

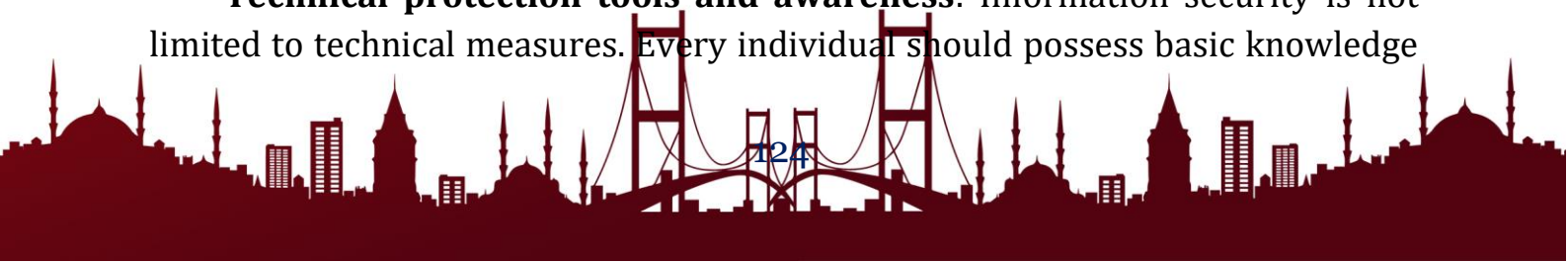
Protection of personal data: As we increasingly use online services, we frequently enter personal data into websites, mobile applications, or online shops. If this information falls into the wrong hands, it may be exploited to steal identities, hack into bank accounts, or commit other serious crimes. For instance, the 2017 Equifax data breach resulted in the theft of personal information from 147 million individuals [3], causing widespread financial harm and prompting reforms in personal data protection policies.

Economic risks for businesses: For enterprises, information security is not only about safeguarding data but also ensuring economic stability. Operations conducted through IT systems are vital for any organization. A breach or theft of internal data can lead not only to financial losses but also irreparable reputational damage. For example, cyberattacks on Yahoo in 2013 and 2014 led to the exposure of over 3 billion user accounts [4].

National security: Information security holds strategic importance for states. If essential data belonging to public institutions and citizens is not protected, malicious groups can exploit this information to undermine governmental structures. This poses a significant threat not only to national security but also to a country's overall stability.

Information manipulation and misinformation: Information security also involves protection from the spread of false information. Today, fake news spreads rapidly through the internet and social media, with bad actors leveraging these tools to manipulate public opinion. An example is deceptive advertising, such as messages claiming a person has won a cash prize, which lure victims into sharing bank details and falling prey to fraud.

Technical protection tools and awareness: Information security is not limited to technical measures. Every individual should possess basic knowledge



of how to protect themselves online. Using strong passwords, avoiding suspicious emails, and regularly backing up data are simple yet crucial steps to protecting personal data.

With the field of cybersecurity rapidly evolving, it is increasingly important for individuals to enhance their digital literacy. Free cybersecurity courses offered by international organizations and universities play a significant role in improving public awareness and capabilities.

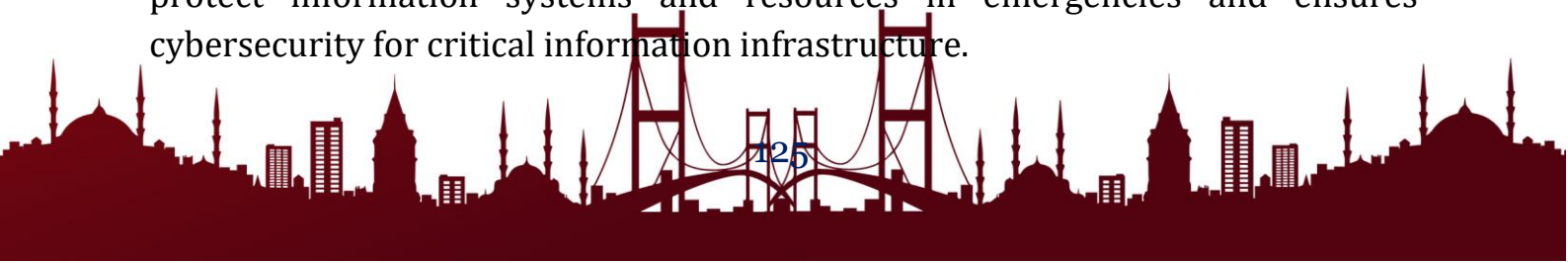
Information security today holds vital significance for every individual, organization, and government. To protect personal data, eliminate economic threats, ensure national security, and guard against disinformation, effective information security measures are essential. By enhancing our understanding and utilizing technical safeguards, we can ensure the integrity and safety of data. Information security is not merely a technical matter—it is a cornerstone of social stability and development.

In Uzbekistan, particular attention is being paid to issues of information and cybersecurity. Laws and regulations are being developed and improved to meet modern challenges. The development of ICT and the necessity to protect the information security and cybersecurity of individuals, society, and the state has become a top national and strategic priority. This requires coordinated efforts from the government and society.

Government ministries, agencies, enterprises, organizations, and businesses are all responsible for ensuring information and cybersecurity, which ultimately serves the national interest. This is especially important in an era where threats to national security increasingly originate from the digital information space.

The cybersecurity sector is regulated by the state. According to Article 10 of the Law of the Republic of Uzbekistan No. O'RQ-764 dated April 15, 2022, "On Cybersecurity", the President of the Republic of Uzbekistan defines the state policy on cybersecurity [5].

The State Security Service of the Republic of Uzbekistan is the authorized government agency in the field of cybersecurity. It is tasked with developing regulatory documents and state programs related to cybersecurity, overseeing the implementation of relevant legislation, conducting intelligence and pre-investigative actions, and organizing preventive and responsive measures against cyber incidents. Additionally, the Service formulates action plans to protect information systems and resources in emergencies and ensures cybersecurity for critical information infrastructure.



To ensure cybersecurity, subjects in this field are granted the right to obtain information from the authorized state body regarding cyber threats, software, hardware and technological vulnerabilities, protection tools and methods, and strategies for identifying and neutralizing cyberattacks. They are also entitled to develop and implement measures for ensuring their own cybersecurity.

References:

1. Constitution of the Republic of Uzbekistan. (2023). Tashkent. <https://lex.uz/docs/6445145>
2. Law of the Republic of Uzbekistan No. O'RQ-547 "On Personal Data" dated July 2, 2019. <https://lex.uz/docs/4396419>
3. Equifax credit bureau to pay \$700 million due to major data breach. Interfax. <https://www.interfax.ru/business/669989>
4. Yahoo announces that the 2013 hacker attack affected 3 billion accounts. TASS. <https://tass.ru/ekonomika/4614220>
5. Law of the Republic of Uzbekistan No. O'RQ-764 "On Cybersecurity" dated April 15, 2022. <https://lex.uz/uz/docs/-5960604>

