

## THE URGENCY OF ENSURING INFORMATION SECURITY

*Saidova Nigina Sirojiddin qizi*[sdvangn21@gmail.com](mailto:sdvangn21@gmail.com)*Master, Faculty of International Law**University of World Economy and Diplomacy/Tashkent/ Uzbekistan*

**Annotation:** this scientific article is based on the theoretical data analysis of the information security system, and highlights the relevance of information security issues in the current era. The main principles of the information security system and the legal measures available in the country are discussed.

**Key words:** information, information security, public information, confidential information, documented information, confidential information.

**Introduction**

As the field of information and communication technologies has developed, in addition to using its advantages and conveniences, ensuring information security is becoming the most urgent issue in our country. This field must definitely develop and we will do it...

*Sh.M. Mirziyoyev*

The development of modern information technologies is observed together with negative events such as industrial espionage, computer crime, unauthorized access, modification, loss of confidential information. Therefore, information protection is an important state task in any country.

The need for information protection in Uzbekistan is reflected in the creation of the state system of information protection and the development of the legal basis of information security. "On Disclosure", "On Preservation of State Secrets", "On Legal Protection of Computer Programs and Databases" and other laws and a number of government decisions were adopted and implemented. Information protection should ensure the prevention of damage caused by voluntary loss of information (theft, tampering, forgery). It is necessary to organize information protection measures based on the current laws and regulatory documents on information security and according to the interests of information users. In order to ensure a high level of information protection, it is necessary to regularly solve complex scientific and technical tasks and improve protection tools.

### Methodology

Information protection should ensure the prevention of damage caused by voluntary loss of information (theft, tampering, forgery). It is necessary to organize information protection measures based on the current laws and regulatory documents on information security and according to the interests of information users. In order to ensure a high level of information protection, it is necessary to regularly solve complex scientific and technical tasks and improve protection tools.

### Data collection and analysis

Information security system- the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.<sup>1</sup>

The basic tenets of information security are confidentiality, integrity and availability. Every element of the information security program must be designed to implement one or more of these principles. Together they are called the CIA Triad:<sup>2</sup>

#### Confidentiality

Confidentiality measures are designed to prevent unauthorized disclosure of information. The purpose of the confidentiality principle is to keep personal information private and to ensure that it is visible and accessible only to those individuals who own it or need it to perform their organizational functions.

#### Integrity

Consistency includes protection against unauthorized changes (additions, deletions, alterations, etc.) to data. The principle of integrity ensures that data is accurate and reliable and is not modified incorrectly, whether accidentally or maliciously.

#### Availability

Availability is the protection of a system's ability to make software systems and data fully available when a user needs it (or at a specified time). The purpose of availability is to make the technology infrastructure, the applications and the data available when they are needed for an organizational process or for an organization's customers.

<sup>1</sup>

[https://csrc.nist.gov/glossary/term/information\\_systems\\_security#:~:text=The%20protection%20of%20information%20systems,document%2C%20and%20counter%20such%20threats.](https://csrc.nist.gov/glossary/term/information_systems_security#:~:text=The%20protection%20of%20information%20systems,document%2C%20and%20counter%20such%20threats.)

<sup>2</sup> [https://www.imperva.com/learn/data-security/information-security-infosec/#:~:text=Information%20security%20\(sometimes%20referred%20to,accessing%20business%20or%20personal%20information.](https://www.imperva.com/learn/data-security/information-security-infosec/#:~:text=Information%20security%20(sometimes%20referred%20to,accessing%20business%20or%20personal%20information.)



These three requirements may be emphasized differently in various applications. For a national defense system, the chief concern may be ensuring the confidentiality of classified information, whereas a funds transfer system may require strong integrity controls. The requirements for applications that are connected to external systems will differ from those for applications without such interconnection. Thus the specific requirements and controls for information security can vary.

The framework within which an organization strives to meet its needs for information security is codified as security policy. A security policy is a concise statement, by those responsible for a system (e.g., senior management), of information values, protection responsibilities, and organizational commitment. One can implement that policy by taking specific actions guided by management control principles and utilizing specific security standards, procedures, and mechanisms. Conversely, the selection of standards, procedures, and mechanisms should be guided by policy to be most effective<sup>3</sup>.

The information security system closely connects the state policy in the information field with the state policy of ensuring national security in the country. In this case, the information security system unites the main organizers of state policy into a single whole. This determines the role of information security and its position in the country's national security system. The totality of goals that reflect the national interests of Uzbekistan in the field of information, the strategic directions of their achievement and the systems of their implementation means the state information policy. At the same time, the state information policy is the main organizer of the country's foreign and domestic policy and covers all aspects of society. The modern concept of information security

<sup>3</sup>National Academies of Sciences, Engineering, and Medicine. 1991. Computers at Risk: Safe Computing in the Information Age. Washington, DC: The National Academies Press. <https://doi.org/10.17226/1581>.

refers to a set of official views on the goals, tasks, principles and main directions that ensure information security. Below are the key elements and aspects of information security:

- information protection (in the sense of protection of personal data, state and service secrets and other types of information whose distribution is limited);
- computer security or data security - a set of hardware and software tools that ensure the storage, access and confidentiality of data in computer networks, measures to protect against unauthorized use of information;
- protection of information and its supporting infrastructure from natural or artificial accidental or intentional impacts that may harm the owners of information or users of information and the infrastructure supporting it;
- protection of the requirements of citizens, separate groups and social strata, the population in general for quality information necessary for their living activities, education and development.

### **Result and discussion**

We use information security to protect valuable information assets from a wide range of threats, including theft, espionage, and cybercrime. Information security is necessary to ensure the confidentiality, integrity, and availability of information, whether it is stored digitally or in other forms such as paper documents. Here are some key reasons why information security is important:

- **Protecting sensitive information:** Information security helps protect sensitive information from being accessed, disclosed, or modified by unauthorized individuals. This includes personal information, financial data, and trade secrets, as well as confidential government and military information.
- **Mitigating risk:** By implementing information security measures, organizations can mitigate the risks associated with cyber threats and other security incidents. This includes minimizing the risk of data breaches, denial-of-service attacks, and other malicious activities.
- **Compliance with regulations:** Many industries and jurisdictions have specific regulations governing the protection of sensitive information. Information security measures help ensure compliance with these regulations, reducing the risk of fines and legal liability.
- **Protecting reputation:** Security breaches can damage an organization's reputation and lead to lost business. Effective information security can help protect an organization's reputation by minimizing the risk of security incidents.
- **Ensuring business continuity:** Information security helps ensure that critical business

functions can continue even in the event of a security incident. This includes maintaining access to key systems and data, and minimizing the impact of any disruptions.<sup>4</sup>

### Conclusion

Information security means the protection of information and the infrastructure supporting it from accidental or intentional effects of a natural or artificial nature. Such impacts can seriously harm information relations, including information owners, information users, and the infrastructure that supports information protection. In the Law of the Republic of Uzbekistan No. 439-II dated December 12, 2002 "On Principles and Guarantees of Information Freedom", information security is defined as information security, and it means the state of protection of the interests of individuals, society and the state in the information field. . In the field of information, personal interests are manifested in the realization of the constitutional rights of citizens regarding the use of information, in engaging in activities not prohibited by law, and in the use of information for physical, spiritual and intellectual development, in the protection of information that ensures personal security. In the field of information, the interests of the society are reflected in the provision of individual interests, strengthening of democracy, construction of social legal state, and support of social solidarity. In the field of information, the state's interests are in creating conditions for the development of the national information infrastructure, in the realization of the constitutional rights and freedoms of individuals and citizens in the field of obtaining information, in the use of information in order to ensure the territorial unity, sovereignty and strength of the constitutional system, political, economic and social stability of Uzbekistan, legality and law is expressed in the strict implementation of order, in the development of international cooperation in mutual equality and mutual interest.

### References

1. Mirziyoev Sh.M. Together we will build a free and prosperous, democratic country of Uzbekistan. Speech at the joint meeting of the chambers of the Oliy Majlis dedicated to the inauguration ceremony of the President of the Republic of Uzbekistan, Tashkent, 2016.566.
2. "Concepts of Information Security." National Research Council. 1991. Computers at Risk: Safe Computing in the Information Age. Washington, DC: The National Academies Press. doi: 10.17226/1581.×

---

<sup>4</sup> <https://www.geeksforgeeks.org/what-is-information-security/>

3. National Academies of Sciences, Engineering, and Medicine. 1991. Computers at Risk: Safe Computing in the Information Age. Washington, DC: The National Academies Press. <https://doi.org/10.17226/1581>.
4. Takhirov Bekhzod Nasriddinovich 'INFORMATION SECURITY FOUNDATIONS' —"SCIENCE AND EDUCATION" certificate number: 307701245. 25.01.2022/Original-layout allowed to click. 28.11.2022
5. Ganiev S. K., Karimov M. M., Tashev K. A. —Information security. Communicator. 2008.
6. [https://csrc.nist.gov/glossary/term/information\\_systems\\_security#:~:text=The%20protect ion%20of%20information%20systems,document%2C%20and%20counter%20such%20t hreats](https://csrc.nist.gov/glossary/term/information_systems_security#:~:text=The%20protect ion%20of%20information%20systems,document%2C%20and%20counter%20such%20t hreats).
7. [https://www.imperva.com/learn/data-security/information-security-infosec/#:~:text=Information%20security%20\(sometimes%20referred%20to,accessing%20business%20or%20personal%20information](https://www.imperva.com/learn/data-security/information-security-infosec/#:~:text=Information%20security%20(sometimes%20referred%20to,accessing%20business%20or%20personal%20information).
8. <https://www.geeksforgeeks.org/what-is-information-security/>