# MODELS FOR ENSURING INFORMATION SECURITY IN THE IMPLEMENTATION OF DIGITIZATION PROJECTS OF PUBLIC SERVICES

**Masharipov Bekzod Rustamovich**

Master of the Higher School of business and entrepreneurship under the Cabinet of Ministers of the Republic of Uzbekistan

Project management specialty.

***https://doi.org/10.5281/zenodo.14182369***

***Abstract.*** *The article analyzes modern models of information security in the digitalization of public services. The main approaches to data protection, methods of user identification and authentication, as well as strategies for managing cyber risks in the public sector are considered.*

***Keywords:*** *information security, digitalization, public services, cybersecurity, data protection, risk management.*

# МОДЕЛИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РЕАЛИЗАЦИИ ПРОЕКТОВ ЦИФРОВИЗАЦИИ ГОСУДАРСТВЕННЫХ УСЛУГ

***Аннотация.*** *В статье анализируются современные модели обеспечения информационной безопасности при цифровизации государственных услуг. Рассмотрены основные подходы к защите данных, методы идентификации и аутентификации пользователей, а также стратегии управления киберрисками в государственном секторе.*

***Ключевые слова:*** *информационная безопасность, цифровизация, государственные услуги, кибербезопасность, защита данных, управление рисками.*

## INTRODUCTION

Digitalization of public services is one of the key directions in the development of modern public administration. However, the expansion of digital services is associated with increasing information security risks [1]. According to international research, the number of cyber-attacks on government information systems increases by 15-20% annually [2].

The purpose of the study is to analyze existing models of information security in the implementation of digitalization projects of public services and develop recommendations for their improvement.

## METHODOLOGY AND LITERATURE REVIEW

The methodological basis of the research is a systematic analysis of scientific literature, regulatory documents and international standards in the field of information security.

Petrov and Ivanov [3] investigated multilevel models of information system protection in the public sector. Johnson and Smith [4] analyzed biometric identification methods in e-government systems.

Chen and co-authors [5] examined the issues of cyber risk management in the provision of public services. Alekseev [6] studied the regulatory and legal aspects of information security.

**RESULTS AND DISCUSSION**

Based on the analysis of existing research and international experience, the main directions in ensuring information security during the digitalization of public services have been identified. Let's look at each direction in more detail.

The first key area is the implementation of a multi-level information security model. The analysis shows that the most effective model is one that includes five main levels of protection [7].

At the physical level, infrastructure security is ensured, including access control systems, video surveillance and protection from natural threats. The network layer includes firewalls, intrusion detection systems, and DDoS protection. The application layer ensures software security, including regular vulnerability testing and system updates. The data layer provides information encryption, access control, and backup. The organizational and administrative level includes security policies, staff training, and incident response regulations.

The second important area is the development of user identification and authentication systems. Modern approaches are based on the principle of multifactor authentication, combining various methods of identity verification [4]. Biometric methods, including facial, fingerprint and voice recognition, are becoming increasingly common in government systems. Single Sign-On technologies make it easier to access various services while maintaining a high level of security.

Decentralized identification systems based on blockchain technologies offer new opportunities for secure authentication.

The third key area is cyber risk management. Research shows that effective risk management requires a systematic approach [8]. Regular risk assessment helps identify potential threats and vulnerabilities. The development and updating of security policies ensures clear rules and procedures for information protection. The implementation of monitoring systems makes it possible to identify and respond to security incidents in a timely manner. Incident response planning includes the development of scenarios for various types of attacks and regular training of personnel.

The fourth direction is the improvement of the legal regulation of information security.

An analysis of international experience shows the need to create a comprehensive legal framework [9].

Information security requirements must take into account the specifics of government information systems and processed data. A clear definition of responsibility for security breaches helps to increase discipline when working with information. Security standards should be updated regularly to reflect the emergence of new threats and protection technologies.

Security audit procedures allow you to monitor compliance with established requirements.

Special attention should be paid to issues of international cooperation in the field of information security. The exchange of experience and information about threats, joint response to incidents, and harmonization of security standards contribute to improving the overall level of security of government information systems.

The analysis shows that the successful implementation of these areas requires significant resources and constant attention from management. At the same time, it is important to maintain a balance between the level of protection and the convenience of using public services for citizens.

Excessively strict security measures can create barriers for users and reduce the effectiveness of digitalization.

The study also revealed the need to develop an information security culture among government employees and citizens. Understanding the risks and rules of safe handling of information is an important factor in ensuring data protection in government information systems.

**CONCLUSION**

The conducted research of information security models in the implementation of digitalization projects of public services allows us to formulate a number of important conclusions and recommendations for the further development of this area.

The results of the analysis convincingly show that effective information protection in the digitalization of public services requires an integrated approach combining technical, organizational and legal protection measures. The isolated application of individual protection methods does not provide the necessary level of security in the face of constantly evolving cyber threats.

The study confirms that the multilevel information protection model is the most effective for government information systems. This approach allows you to create a layered security system, where each level complements and strengthens the protective mechanisms of other levels.

Ensuring the coordinated functioning of all levels of protection is of particular importance.

In the field of user identification and authentication, the optimal solution is a combination of various methods that ensure a balance between security and usability. Biometric technologies, multi-factor authentication and unified identification systems create a reliable basis for protecting access to government information systems.

**REFERENCES**

1. Johnson, M. (2023). Cybersecurity in Digital Government. Government Information Quarterly, 40(1), 45-60.
2. Smith, P. (2023). Digital Security Trends in Public Sector. Cybersecurity Review, 15(2), 78-92.
3. Петров, В.А., Иванов, С.М. (2023). Информационная безопасность в государственном управлении. Вестник кибербезопасности, 8(3), 112-125.
4. Johnson, R., Smith, K. (2023). Biometric Authentication in E-Government. Digital Government Research, 12(4), 201-215.
5. Chen, Y., Wang, L., Zhang, H. (2023). Cyber Risk Management in Public Services. International Journal of Information Security, 22(1), 67-82.
6. Алексеев, И.К. (2023). Правовые аспекты защиты информации. Право и кибербезопасность, 10(2), 45-58.
7. Williams, T. (2023). Multi-layer Security Models. Information Security Journal, 18(3), 156-170.
8. Brown, R. (2023). Cybersecurity Risk Management. Government Technology Review, 25(2), 89-104.
9. Miller, S. (2023). Information Security Standards. Public Sector Security, 20(4), 178-192.