AJLISI
GLOBAL RESEARCH NETWORK

Information Horizons: AMERICAN Journal of Library and Information Science Innovation
Volume 01, Issue 09, 2023 ISSN (E): 2993-2777

Methods And Means Of Protecting The Database Of State Bodies Services From Information Security Risks|

Iminova Husniyahon Khusniddin kizi
Deputy dean, MMFI National Research Nuclear University in Tashkent

Abstract. *In today's digital era, the protection of sensitive information has become a crucial aspect for state bodies and their databases. With the increased reliance on technology, information security risks have also escalated, demanding comprehensive measures to safeguard these databases from unauthorized access, data breaches, and other potential threats. This article explores various methods and means employed by state bodies to protect their database services from information security risks.*

Keywords: *information security,databse,resources,information protection*

Introduction

It is known that the information resources of any country is one of the factors that determine the economic and military potential. Effective use of this resource ensures the country's security and the successful formation of a democratic information society. In such a society, the speed of information exchange increases, the use of advanced information and communication technologies for the collection, storage, processing and use of information is carried out on a large scale.

Information society is forming rapidly. In the world of information, the concept of state borders has disappeared. The global computer network is fundamentally changing public administration. In our daily life, regardless of geographical location various types of information entered through the Internet.

That is why protection against problems such as illegal access to existing information, its use, alteration, and loss has become an urgent issue. State policy in the field of information is the development and improvement of information resources, information technologies and information systems in the modern world.

Information protection, information security and its modern concept The Law of the Republic of Uzbekistan dated December 12, 2002 No. 439-II "On Principles and Guarantees of Freedom of Information" contains definitions of information and its types:

Information - information about persons, objects, facts, events, events and processes, regardless of their sources and form of presentation:

Information protection - measures to prevent threats to information security and eliminate their consequences;

Documented information, audiovisual and other messages and materials intended for public information:

Documented information is information recorded on a material body with requisites that allow identification:

Confidential information - documented information, the use of which is restricted in accordance with legal documents.

This definition of the Cabinet of Ministers of the Republic of Uzbekistan is according to the

decision of the President of the Republic of Uzbekistan No. 296 of November 7, 2011 "On measures to implement the decision No. PK-1572 of July 8, 2011 "On additional measures to protect national information resources" expressed: confidential information, use is limited in accordance with the legal documents of the Republic of Uzbekistan.

Information security threat objects:

All types of information resources containing state secrets, confidential information, commercial secrets, confidential information and other information;

Information systems, technical tools, automated control systems, communication and data transmission systems that receive, store, transmit and process restricted information;

A complex of technical means and buildings for reception, transmission and processing of limited-use information;

Information protection guidelines

Legal protection - protection of information on a legal basis special laws providing, other regulations documents, rules, procedures and activities;

organizational protection - to do some harm to the performers regulations that reduce or prevent based performer collaboration and production regulation of activities;

engineering and technical protection - damage to commercial activity from various technical means that prevent delivery use;

Protecting the database of state bodies' services from information security risks is crucial to ensure the confidentiality, integrity, and availability of sensitive government data. Here are some methods and means that can be adopted to enhance the security of these databases:

Access Control: Implement strict access control mechanisms to restrict unauthorized access to the database. This includes user authentication, role-based access control, and regular monitoring of user activities.

Encryption: Encrypt the data stored in the database to safeguard it from unauthorized access, both at rest and in transit. Strong encryption algorithms should be used to protect sensitive information.

Regular Data Backups: Regularly back up the database to ensure that data can be restored in the event of a security breach or data loss. These backups should be stored securely, with appropriate access controls and encryption.

Patch Management: Stay up-to-date with security patches and updates for the database software. Install patches promptly to address any identified vulnerabilities and protect against potential exploits.

Database Monitoring: Employ intrusion detection systems and database activity monitoring tools to detect and prevent unauthorized access or suspicious activities within the database environment.

Secure Network Infrastructure: Implement firewalls, intrusion prevention systems, and other network security measures to protect the database from external threats and unauthorized network access attempts.

User Training and Awareness: Conduct regular training sessions for employees and users responsible for accessing the database. Educate them on best practices in information security, such as creating strong passwords, recognizing phishing attempts, and reporting suspicious activities.

Incident Response Plan: Develop a robust incident response plan that outlines the steps to be taken in the event of a security breach or incident. This plan should include procedures for data recovery, communication protocols, and collaboration with law enforcement agencies, if necessary.

Auditing and Logging: Enable comprehensive auditing and logging features to track and monitor user activities within the database environment. Review these logs periodically to identify any abnormal activities and potential security breaches.

Physical Security: Ensure physical security measures are in place to protect the server rooms or

data centers where the database is stored. This includes secure access controls, video surveillance, and environmental monitoring systems.

Regular Security Assessments: Conduct periodic security assessments and vulnerability scans to identify any weaknesses or vulnerabilities in the database environment. Remediate any identified issues promptly to maintain a secure database infrastructure. Implementing these methods and means can significantly enhance the security of state bodies' services databases and mitigate information security risks. It is important to review and update these security measures regularly to stay up-to-date with the evolving threat landscape.

Conclusions

Protecting the databases of state bodies from information security risks is an ongoing and multifaceted challenge. Employing robust access control measures, implementing data encryption and secure communication channels, establishing regular data backups, utilizing intrusion detection and prevention systems, and fostering employee awareness are critical elements in successfully safeguarding these databases. By investing in comprehensive information security strategies, state bodies can ensure the confidentiality, integrity, and availability of their services, thereby enhancing public trust and safeguarding sensitive information.

References:

1. Hershey P, Silo C (2012) Procedure for detection of and response to distributed denial of service cyber attacks on complex enterprise systems. In Proceedings of 6th Annual International Systems Conference, Vancouver, 19–22 March 2012, p 85–90
2. NIST Computer Security Division (2006) Guide for developing security plans for federal information systems, NIST SP 800-18. rev Accessed 31 My 2017
3. NIST Computer Security Division (2006) Minimum security requirements for federal information and information systems, FIPS 200. Accessed 31 May 2017
4. Snyder D, et al. Improving the cybersecurity of U.S. air force military systems throughout their life cycles. Santa Monica, CA: Rand Corporation Research Report; 2015.