European Journal of Innovation in Nonformal Education (EJINE)
Volume 4 | Issue 12 | Dec - 2024 ISSN: 2795-8612

Ensuring Information Security in Libraries

Durdonaxon Ubaydullayeva, Ikromjon Habibjonov
Fergana regional branch of Uzbekistan State Institute of Arts and Culture

A B S T R A C T
This article discusses the main tools and methods for ensuring information security in libraries. It explores the role of modern technologies in maintaining information security, including software, privacy policies, and data protection systems. Ensuring information security in libraries not only preserves the integrity and confidentiality of information but also helps increase user trust in the data.

A R T I C L E I N F O
Article history:
Received 04 Nov 2024
Received in revised form
05 Nov 2024
Accepted 21 Dec 2024

Keywords: libraries, information security, protection tools, modern technologies, software, privacy policies, data protection, integrity, confidentiality, user trust.

Hosting by Innovatus Publishing Co. All rights reserved. © 2024

Ensuring information security in libraries is a set of measures undertaken by the institution to protect information resources, user data, and systems. Both technological tools and administrative measures work together to ensure information security. Below is a detailed explanation of the primary tools used to ensure information security in libraries.

1. Technological Tools:

Encryption: A technology used to keep information confidential and prevent its theft during transmission. Encryption ensures that data can only be read by individuals with the proper authorization.

Transport Layer Encryption (TLS/SSL): these protocols encrypt the data transfer process between users and servers when accessing library websites or online resources. HTTPS (Hypertext Transfer Protocol Secure) is a widely used form of this protocol that ensures data security on the internet. Data Storage Encryption: electronic resources stored in library systems (e.g., e -books, articles, user data) must be encrypted to ensure their complete security. Firewalls: used to protect systems and networks from external attacks and malicious software. Firewalls secure the library's network and prevent unauthorized access. Internal and External Firewalls: libraries typically install firewalls between their internal network and the external network. These firewalls allow necessary traffic while blocking harmful actions and illegal access. Antivirus and Anti-malware Software: these programs are used to detect and prevent malicious software in library systems. They prevent harmful programs such as viruses, trojans, and spam from entering user computers and systems. Regular Updates: keeping antivirus systems updated allows for the detection and blocking of new malicious programs. Network Activity Monitoring: monitoring network activity is a critical tool in ensuring the security of library systems. Network monitoring helps detect suspicious or dangerous activity, allowing for necessary actions. Intrusion Detection System (IDS) and Intrusion Prevention System (IPS): IDS detects potential threats in the network, while IPS stops them and automatically takes protective measures when necessary.

Data Backup: A crucial tool for ensuring the security of information stored in libraries. Backups allow for the restoration of lost or damaged data. Libraries regularly create backup copies of electronic resources,

user data, and system settings. Cloud Storage: data can be securely and efficiently stored in cloud services, providing easy and safe access.

2. User Access Control Tools: the primary tools for managing user access to systems are authentication and authorization processes. Authentication confirms the identity of a user, and authorization determines what resources they can access.

Password Authentication: users must enter their secret password to access the system. Setting complex and secure passwords protects users' accounts. Two-factor Authentication (2FA): after entering the password, users must also enter a code sent to their phone as an additional security measure. Libraries assign users access rights based on roles and permissions within the system. This ensures that each user only has access to necessary resources, increasing system security. Access to Data: some users may only have reading rights, while others may have the right to edit or add data.

3. Data Storage and Protection Tools: all information stored in library systems (e.g., e-books, articles, user data) must be kept encrypted. This encryption protects against data theft or misuse. Libraries must regularly update the software they use to protect it from malicious users. Software updates enhance system security. Software Updates: Libraries need to update systems and software regularly, as updates are often aimed at improving security.
4. Staff Training and Awareness: training library staff and users in information security is also an important tool. This helps them learn how to protect against malicious software, phishing attacks, and other threats. Training and Seminars: regular training should be conducted for staff on security policies, data protection, and system access management.

In conclusion, libraries need to implement a set of measures in technological, administrative, and data protection areas to ensure information security. This not only protects library systems but also helps to securely store user data and resources. Additionally, regular training of staff and users in information security ensures the effective and secure operation of library systems. This approach enhances trust and efficiency in library information security. Information security is important for libraries not only from a technological standpoint but also from a legal and ethical perspective. Libraries must ensure information security in their services to protect users' data and safeguard against global threats. Regular training of staff and users in information security, updating systems and resources, and monitoring security help maintain a high level of security in libraries. This, in turn, increases the reliability, effectiveness, and trust of library users.

References

1. Rasulov, D. (2020). Information Security: Theory and Practice. Tashkent: Uzbekistan Information Publishing.
2. Akhmedov, B. (2018). Ensuring Information Security in Libraries. Samarkand: Samarkand State University Publishing.
3. Ismailov, F. (2019). Modern Information Systems and Security Management. Tashkent: National University Publishing.
4. Mavlonov, S. (2021). Data Protection in Libraries. Bukhara: Bukhara State University Publishing.
5. Karimov, A. (2022). Information Security: Technologies and Strategies. Fergana: Fergana State University Publishing.