ISSN 3060-4567

CYBERSECURITY AND ITS CONCEPT

Qo'qon davlat universtiteti

Xorijiy filalogiya fakulteti

105-25 guruh talabasi

Nabixo'jayeva Mukammalxon

O'qituvchi: ***Abdupattayev Xasanboy***

Annotation: *This article provides a comprehensive explanation of cybersecurity and its connection to media literacy and information culture. It explores essential security principles, modern digital threats, and practical strategies users can apply to protect personal data and evaluate online information critically.*

Key Words: *Confidentiality* — keeping information secret and ensuring only authorised people can access it.*

**Integrity* — ensuring information is accurate and has not been tampered with.*

**Availability* — ensuring information and services are accessible when needed.*

**Authentication* — verifying the identity of users or systems.*

**Authorization*— granting permissions to perform actions or access resources.*

Introduction: Cybersecurity is the practice of protecting computers, networks, programs, and data from unauthorized access, damage, or theft. In the context of media literacy and information literacy, cybersecurity helps people understand how digital information is created, shared, and protected. It also teaches how to evaluate the trustworthiness of information and how to stay safe while using online media. Modern media and information ecosystems rely heavily on digital platforms. News, social networks, messaging apps, blogs, and streaming services all depend on data and online systems. When these systems are vulnerable, personal

ISSN 3060-4567

privacy and public trust can be harmed. For students and media consumers, understanding cybersecurity is part of evaluating sources, recognizing manipulated content, and protecting oneself from misinformation, scams, and identity theft.

These ideas form the foundation for thinking critically about digital media and for practical safety steps when handling information. For example, Network security protects the infrastructure that connects devices and systems. It includes firewalls, intrusion detection systems (IDS), virtual private networks (VPNs), and secure network design. For media literacy, network security helps ensure that the information you access online has been delivered through safe channels and has not been intercepted or altered in transit. Information security focuses on protecting data in all forms — stored, processed, or transmitted. InfoSec uses encryption, access controls, backups, and policies to protect sensitive data such as personal records, passwords, or confidential reports. In evaluating media sources, InfoSec awareness helps users understand why some data must remain private and why secure handling of sources matters. Application security involves securing software from threats throughout its lifecycle. This includes secure coding practices, regular updates and patches, application testing, and protecting web and mobile apps from common attacks (e.g., SQL injection, cross-site scripting). For information consumers, application security is important because many platforms that publish or host media are applications that may have vulnerabilities. Endpoints are individual devices like smartphones, laptops, and tablets. Endpoint security protects these devices through antivirus software, endpoint detection and response (EDR), disk encryption, and device management. Since most media consumption happens on endpoints, keeping them secure prevents malware from stealing credentials or altering what users see. Cloud security protects data and services hosted by cloud providers. It includes strong access controls, encryption, secure configurations, and shared responsibility models. As more media and information services move to the cloud, understanding cloud security helps users assess the trustworthiness of platforms and how their data might be handled. IAM systems control who can access resources and what they can do. Common measures include multi-factor authentication (MFA), single sign-on

ISSN 3060-4567

(SSO), role-based access control (RBAC), and strong password policies. For media literacy, IAM teaches users how to protect their accounts and verify authentic sources when authentication is required. Operational security covers the policies, procedures, and actions organizations take to protect information during everyday operations. Examples include staff training, incident response planning, and secure communication practices. For media and information professionals, OpSec ensures that sensitive reporting, source identities, and unpublished material remain safe. This area focuses on detecting, analyzing, and responding to cyber incidents, and on conducting forensic investigations afterward. Incident response teams help contain attacks, recover systems, and learn lessons to prevent repeats. Journalists and educators benefit when they understand how incidents may affect media reliability and the provenance of information.

Practical Steps for Individuals

1. **Use strong, unique passwords** and a password manager to store them.
2. **Enable multi-factor authentication (MFA)** on important accounts.
3. **Keep devices and applications updated** with security patches.
4. **Be cautious with links and attachments** in emails and messages; verify senders.
5. **Check the source of information** — prefer primary sources, trusted media outlets, and official documents.
6. **Use secure connections** (look for HTTPS) and avoid using open public Wi-Fi for sensitive activities, or use a VPN if necessary.
7. **Back up important data** regularly and verify backups.
8. **Limit sharing of personal information** on public profiles and be mindful of privacy settings. Teach the basics of cybersecurity** alongside media literacy: explain confidentiality, integrity, availability, and common threats. Include hands-on activities**: recognizing phishing, verifying source authenticity, and checking metadata. Adopt secure workflows** for handling sensitive information,

including encrypted communication for sources when necessary. Develop incident response plans for media organizations and schools, and run tabletop exercises.

Use trusted tools and platforms and vet third-party services for privacy and security practices. Cybersecurity and media literacy intersect strongly when it comes to misinformation. Attacks such as deepfakes, account takeovers, and coordinated disinformation campaigns can manipulate what audiences believe. By combining technical safeguards (e.g., platform security measures, account protections) with critical evaluation skills (e.g., cross-checking, source evaluation), media consumers can reduce the influence of manipulated content.

To sup up ,Cybersecurity is not only a technical field for IT professionals — it is an essential part of media literacy and information literacy. Knowing how information is protected, how systems can be attacked, and what practical steps to take empowers individuals to use media responsibly and safely. Whether you are a student, educator, journalist, or everyday media consumer, integrating cybersecurity knowledge into media literacy practice strengthens trust, privacy, and the overall health of information ecosystems.

OFFICIAL SOURCES AND LITERATURE USED

NIST (National Institute of Standards and Technology) — Cybersecurity Framework and Special Publications (e.g., NIST SP 800-series).

1. **ISO/IEC 27001 and ISO/IEC 27002** — International standards for information security management systems.
2. **ENISA (European Union Agency for Cybersecurity)** — Reports and guidance on cybersecurity best practices.
3. **OWASP (Open Web Application Security Project)** — OWASP Top Ten and application security resources.
4. **CERT/CC (Computer Emergency Response Team Coordination Center)** — Advisories and incident handling guidance.
5. **Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*.**
6. **Bishop, M. (2003). *Computer Security: Art and Science*.**

ISSN 3060-4567

7. **ISO/IEC and national cybersecurity strategy documents** published by education and government agencies.