MECHANISMS FOR ENSURING INFORMATION SECURITY IN INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SERVICES

Shahboz Shodi Rajaboyev
Samarkand Institute of Economics and Service, Assistant of the Department of "Information Technologies"
ORCID: 0000-0002-0997-6689
Diyorbek Ibratovich Ishmuratov
Student, Samarkand Institute of Economics and Service

Annotation. This article is devoted to studying the technical, organizational, and legal mechanisms for ensuring information security in information and communication technology (ICT) services. The article analyzes the core principles of security—confidentiality, integrity, and availability—as well as real threats, cyberattacks, and protection strategies against them.

Keywords: information and communication technologies, ICT services, information security, data protection, cybersecurity, digital transformation, technological infrastructure, digital culture.

Introduction

Today, information and communication technologies (ICT) have become an integral part of social development and the management system. With the expansion of digitalization, the daily activities of government agencies, educational institutions, banking and financial systems, the healthcare sector, and business entities can no longer be imagined without ICT services. The primary purpose of ICT services is to increase the efficiency of information exchange, optimize organizational processes, and improve the management of large-scale economic and social activities.

However, as ICT services expand, the associated risks are also sharply increasing. In particular, cyberattacks, the illegal dissemination of personal data, information theft, the misuse of artificial intelligence for harmful purposes, and the disruption of state information systems have become some of the major challenges of the modern world. Ensuring the security of such ICT services has direct strategic importance for national, economic, political, and social stability.

The deepening of digital transformation processes is significantly increasing the demand for ICT services. However, along with this process, threats related to information protection—such as cyberattacks, malware, and the leakage of personal data—are becoming more intensive.

Therefore, the improvement of information security mechanisms in ICT services is becoming an urgent and essential task.

Main Part. Theoretical Foundations of Information Security in ICT Services

Information security is based on **three core principles**, commonly known as the CIA triad:

1. **Confidentiality**
2. **Integrity**
3. **Availability**

Confidentiality

The principle of confidentiality ensures that information is accessed only by authorized individuals by restricting unauthorized access. At the core of this principle lie access control mechanisms, processes for identification and authentication, encryption methods, and strict definition of access levels. Maintaining confidentiality helps organizations prevent data leakage caused by internal and external threats, ensuring the constant protection of users' personal information, financial records, and operational resources.

Integrity

The integrity principle protects the accuracy, correctness, and immutability of information. This means that data must not be altered without authorization during transmission or storage.
To support this principle, cryptographic hash functions, digital signatures, transaction verification mechanisms, logging systems, and audit tools are utilized. Ensuring integrity is critically important for government institutions, the banking sector, healthcare organizations, and many other fields, as even minor inaccuracies in data can significantly affect decision-making processes.

Availability

The principle of availability ensures that information resources, services, and systems are continuously accessible when needed. System availability requires resilience against attacks, technical failures, power outages, or overloads. To ensure availability, data backups, disaster recovery plans, load balancing, DDoS protection mechanisms, and high-reliability server infrastructure are implemented.
Guaranteeing availability ensures the continuity of economic, social, and governmental services and creates a reliable service environment for users.

The three principles described above are summarized in **Table 1**.

Core Principles of Information Security

Principle	Description
Confidentiality	Ensuring that information is accessible only to authorized users.
Integrity	Ensuring that information is accurate, unaltered, and protected from unauthorized modification.
Availability	Ensuring continuous and timely access to systems and data when needed.

Consequences of Violating These Principles, Practical Examples, and Comparative Analysis

1. Confidentiality Violation

When confidentiality is compromised, information falls into the hands of unauthorized individuals. This leads not only to the exposure of personal data but also to fraud, financial losses, and a decline in trust during service delivery. In corporate environments, a breach of confidentiality may result in the leakage of trade secrets, unlawful use of information by competitors, and severe damage to brand reputation.

Practical examples:

- Large-scale leakage of social network user data due to unencrypted password storage.
- Personal data from government registries being exposed online.

2. Integrity Violation

Integrity breaches cause the loss of data accuracy and reliability. This is particularly dangerous for sectors such as banking, healthcare, transportation management, and government registries.
Even a tiny unauthorized modification can result in incorrect decisions, distorted financial balances, or disruption of operational processes.

Practical examples:

- Unauthorized alterations to transaction records in a bank database, causing customer account balances to display incorrectly.
- Illegal modification of medical test results leading to an incorrect diagnosis.

3. Availability Violation

When availability is compromised, information resources become temporarily or permanently inaccessible. This leads to service outages, economic damage, slower government operations, and the inability of citizens to access essential services.

Practical examples:

- A DDoS attack on an online payment system causing banking services to remain unavailable for several hours.
- Failure of internal systems due to lack of backups after a server malfunction.

Threats to ICT Services

As ICT services expand, the threats targeting them grow in complexity and scale. These threats affect not only organizational infrastructure but also critical sectors such as government administration, banking and finance, education, and healthcare.

Cyberattacks

Cyberattacks in the digital space are increasing annually. According to Cybersecurity Ventures, cybercrime caused **9.5 trillion USD** in global losses in 2024. Such attacks pose a serious threat to the continuity of ICT services.

Most Common Attacks

- **DDoS attacks** – disrupting services by overwhelming networks. The largest DDoS attack recorded in 2023 reached **71 million requests per second**.
- **Phishing** – deceiving users into revealing confidential data. Phishing attacks in the manufacturing sector increased by **76%** over the last three years.
- **Malware** – ransomware, spyware, and trojans that encrypt or steal data.

Insider Threats

Internal threats are often overlooked but remain highly dangerous. According to IBM Security, **21%** of all data breaches are linked to insider activity.

Types:

- **Unintentional errors** – mistakes by untrained employees, misconfigurations, accidental data deletion.
- **Intentional harm** – disgruntled employees leaking passwords, stealing data, or exploiting excessive privileges.

These threats significantly endanger databases, servers, and e-government platforms.

Weak Infrastructure and Delayed Updates

Outdated servers, unsupported operating systems, and irregular updates increase vulnerability.
Microsoft's 2024 report states that **57%** of successful cyberattacks occurred because patches were not applied on time.

Social Engineering

Even with strong technical protection, the human factor remains the weakest link. Through social engineering:

- fake calls (tech support scams),
- identity impersonation,
- manipulative emails,

users unknowingly compromise the system.
According to the 2023 Verizon Data Report, **74%** of breaches involved human error.

Information Security Strategies

As digital services become central to social and economic life, developing strong information security strategies has become a priority. Modern threats go beyond viruses and hacking—they include employee errors, misconfigurations, cloud failures, and even global infrastructure disruptions.
Therefore, ensuring security is not a one-time measure but a continuous and comprehensive process.

1. Multi-Layer Security Architecture

Relying on a single security tool is a serious risk.
Verizon's 2023 analysis found that **62%** of breaches occurred because attackers bypassed multiple protection layers.
Thus, networks, servers, applications, user devices, and data must each have their own dedicated protection mechanisms.

2. Strengthening Cryptographic and Authentication Systems

Advanced encryption algorithms, mandatory two-factor authentication (2FA), and biometric identification significantly improve confidentiality and

integrity.
According to Microsoft, 2FA prevents **up to 99%** of automated attacks targeting user accounts.

3. Improving Employee Cyber Hygiene

Globally, **35–40%** of cyber incidents occur due to employee negligence. Regular training, phishing detection exercises, and strict password policies become essential components of a strong security system.

4. Enhancing Monitoring and Incident Response

Real-time log monitoring, AI-based anomaly detection, and rapid-response teams reduce attack damage significantly.
IBM Security reports that organizations with incident-response systems reduce breach costs by **about 30%**.

All strategies must work together as an integrated system. The future resilience of organizations depends on how consistently and continuously these approaches are implemented.

Table 2. Mechanisms for Ensuring Information Security

Mechanism Type	Basic Description	Expanded Notes
Technical mechanisms	Encryption algorithms, firewalls, antivirus systems, network monitoring, access control, DDoS protection, backup and recovery systems.	Zero Trust architecture, SIEM, IDS/IPS, MFA, cloud security scanners, key management systems (KMS), EDR/XDR.
Organizational mechanisms	Security policies, employee training, emergency preparedness plans.	Internal policies, risk management, employee certification (Security+, CEH, CHFI), audits, password policy, RBAC, SOC establishment.
Legal mechanisms	ICT laws of Uzbekistan, ISO/IEC 27001, cybersecurity regulations.	Uzbekistan's Cybersecurity Concept, GDPR, NIST SP 800-53, Data Protection Agreements (DPA), formal privacy policies, certification requirements.

Conclusion

Ensuring information security in ICT services requires a combination of technical, organizational, and legal mechanisms. Security is effective not just through protective tools but through comprehensive management and monitoring frameworks. Research confirms that ICT services form the backbone of modern socio-economic systems, and their stability is crucial for government operations, business processes, and societal safety.

The core security principles—confidentiality, integrity, and availability—remain central components. Growing threats demand advanced approaches: multi-layer security architecture, cryptographic technologies, employee cyber hygiene, and improved monitoring and incident response systems.

Ultimately, maintaining information security in ICT services depends on systematic, continuous, and strategic management rather than isolated tools. The efficiency of digital transformation, organizational resilience, and protection against cyber risks are all determined by how well these approaches are implemented.

References

1. Boronov, B., & Mukhammadiev, Z. (2025). *Ways to Expand the Information Volume of Accounting for Capital Investments in Economic Entities*. Advanced Economics and Pedagogical Technologies, 2(2), 444–450. Retrieved from https://inlibrary.uz/index.php/aept/article/view/80274
2. Rajaboev, Sh. Sh. *Digitalization and the Green Sector in Sustainable Development*. BBK 65.05 P 78, p. 596.
3. Boronov, B., & Salomov, Sh. (2025). *Organizational and Legal Aspects of the Development of Non-State Educational Organizations*. Economic Development and Analysis, 3(2), 268–274. Retrieved from https://inlibrary.uz/index.php/eitt/article/view/80115
4. Rajaboev, S. S. *Technologies of Using Multimedia Tools in Teaching Economic Sciences*. Spanish Journal of Innovation and Integrity.
5. Boronov, B. F., Akhmedov, M. A., & Khudaynazarova, D. G. (2024). *Issues of Reflecting Revenues and Expenses in the Statement of Other Comprehensive Income in Enterprises*. Economics and Society, 3-2(118), 547–556.
6. Boronov, B. F., & Mustafayev, A. F. (2024). *Organizational Issues of Developing Non-State Educational Services*. Economics and Society, 5-2(120), 926–929.
7. Rajaboev, Sh. Sh. (2022). *The Role of Information Technologies in Technological Entrepreneurship*. BBK 65.29 ya43 T384, p. 54.