AL-FARABI KAZAKH NATIONAL UNIVERSITY

FACULTY OF INFORMATION TECHNOLOGY AND ARTIFICIAL INTELLIGENCE
DEPARTMENT OF CYBERSECURITY AND CRYPTOLOGY

LEGAL REGULATION OF INFORMATION SECURITY

Lecturer: PhD, Acting Associate Professor Assem Turarbek

MODULE 1

INFORMATION SECURITY AND ELECTRONIC SERVICES

LECTURE 1

THE CONCEPT OF INFORMATION SECURITY

LECTURE OBJECTIVE

Explain the main properties of information security, distinguish protection measures from security objectives and describe the role of state regulation.

LECTURE PLAN

1. Information assets and the CIA triad

2. Authenticity, accountability and access

3. State regulation and protection measures

INFORMATION AS AN ASSET

Concept or participant	Meaning, duties and application
Information	Individuals, organizations and public bodies rely on information to make decisions and deliver services.
Information lifecycle	Protection covers collection, processing, storage, use and transmission.
Sources of harm	Deliberate misuse, human error and equipment failure can expose data or interrupt a service.
Prevention and recovery	Controls reduce the likelihood of loss. Detection and recovery limit the harm when an incident occurs.

Information can have value for the person it describes, for the organization that processes it and for public administration. The same resource may pass through several systems. A loss at any stage can affect later decisions, so the scope of protection includes the complete processing environment and the people using it.

CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

Concept or participant	Meaning, duties and application
Confidentiality	Only authorized people can view or receive information. A patient record disclosed to the wrong person loses confidentiality.
Integrity	Data remains accurate and complete. An unauthorized change to a bank balance compromises integrity.
Availability	Authorized users can reach information or services when needed. An outage in a ticketing system affects availability.

The three properties often interact. An unauthorized change can make a service unavailable, while a failed recovery can expose confidential data. The appropriate control depends on the resource and its purpose. A public timetable chiefly needs reliable content and availability, while a medical record also requires strict limits on disclosure.

AUTHENTICITY AND NON-REPUDIATION

Concept or participant	Meaning, duties and application
Authenticity	Evidence supports the claimed origin of a message or action. A valid digital signature can help verify who signed a document.
Non-repudiation	Records can support proof of an action if its author later disputes it. A signed document and a timestamped record can help establish what happened.
Audit trail	An event record links an action to an account, time and outcome. Its value depends on the integrity of the logs and the strength of identity checks.

A signature, timestamp and activity log answer different questions about an action. The signature supports verification of the signed content and signer, the timestamp places the action in time, and the log records system activity. The quality of the evidence depends on protecting each record against unauthorized modification.

IDENTITY AND ACCESS IN ICT SYSTEMS

Identification

The user presents an identifier, such as a university account name.

Authentication

The system verifies the claimed identity using a password, security key or another credential.

Authorization

The system checks what the authenticated user is allowed to do. A lecturer may edit grades only for assigned courses.

Accountability

The system records actions so that changes can be reviewed later.

Access control continues after login. The system checks permissions during the session, records significant operations and responds when an account’s role changes. Sharing credentials weakens accountability because several people can act under one identifier. Separate accounts and controlled permissions make activity easier to attribute and review.

PRINCIPLES OF STATE REGULATION

Legality and equality

Participants operate within the law and have equal rights to take part in informatization activities.

Rights and legitimate interests

Regulation protects the rights of individuals and legal entities when they use ICT.

Openness of public information

Information about public bodies is generally accessible, subject to legal restrictions. Published information is expected to be timely, complete and reliable.

Common standards

Uniform requirements support reliable systems and centralized management of e-government resources.

Public access to state information depends on its legal category. Published resources need timely updates, complete content and protection against unauthorized alteration. Common standards also support reliability and manageability across different public systems. These principles connect citizens' access to information with the quality and security of the service that provides it.

STATE PRIORITIES IN INFORMATIZATION

Public services

Develop e-government and digital services at the local level.

Digital literacy

Expand access to electronic learning resources and develop ICT skills.

Infrastructure and industry

Support domestic ICT development and protect state resources, systems and networks.

Incident response

Monitor security, prevent incidents where possible and coordinate response. International cooperation supports information exchange.

State priorities include digital literacy, electronic learning, domestic ICT development and investment. Protection of state resources also involves cooperation between public bodies and participation in international information exchange. Incident preparedness extends to social, natural and technological emergencies because such events can interrupt communication and public services.

INFORMATION SECURITY, CYBERSECURITY AND PROTECTION

Information security

The broad field of protecting information and its use across formats and environments.

Cybersecurity

Protection of electronic information and the systems, networks and infrastructure that handle it.

Information protection

Practical measures such as physical security, access controls, cryptography and internal procedures.

Physical measures protect facilities and media. Software and hardware controls regulate access and processing. Cryptography protects information in defined uses, while administrative rules assign responsibilities. Each measure addresses part of the risk. Its effectiveness also depends on correct operation, review and the ability to restore affected resources.

CASE DISCUSSION

A student portal exposes a grade sheet to all users. One grade is then changed, and the portal becomes unavailable during enrolment.

Which event affects confidentiality, which affects integrity, and which affects availability?

What identity and activity records would help investigate the grade change?

Analysis

Disclosure affects confidentiality, the changed grade affects integrity and the outage affects availability. Examine authentication events and the grade-change audit record. Legal duties and practical controls work together to protect information.

STATE REGULATION AND PUBLIC INFORMATION

Public electronic resources support accountability and access to information about public bodies. Openness also creates a duty to preserve the reliability of published information. An openly accessible document still needs protection against unauthorized changes.

The principles in the lecture include legality, equal participation, respect for rights, freedom to search and transmit unrestricted information, and fair competition in ICT. Restrictions on access depend on the applicable legal regime.

During collection, the organization establishes why it needs the information and who may submit it. During processing, permissions and validation rules limit changes. Storage controls protect retained records and support recovery.

Transmission introduces additional risks because information passes between systems and organizations. The recipient, communication channel and record of transfer all matter. Destruction or anonymization closes the lifecycle when retention is no longer justified.

CRITICAL SERVICES AND AVAILABILITY

The lecture uses air traffic control and electricity supply to illustrate systems where uninterrupted operation and accurate data are especially important. A change to operational information can affect both integrity and the availability of a service.

Availability also matters in ticketing, banking and online commerce. An authorized user may be unable to complete a transaction because the service is blocked, its records are damaged or access settings have changed.

A username identifies the account. A password or additional factor provides evidence that the person controls the associated credential. Role assignments determine which records that account can read or change.

An audit record links the account to an action and time. Investigators also need to assess credential sharing, compromised sessions and the protection of the logs before linking the activity to a particular person.

CONCLUSION

1. Confidentiality controls disclosure, integrity protects accuracy and availability preserves authorized access.

2. Identity checks, access permissions and records support accountability.

3. Legal duties and practical controls work together to protect information.

Self-assessment questions

1. What are confidentiality, integrity and availability?
2. How do identification, authentication and authorization differ?
3. What types of threats can affect information throughout its lifecycle?
4. How do legal, organizational and technical measures complement one another?
5. Why is accountability important for information security?

REFERENCES

1. Lecture 1. The Concept of Information Security. Course materials.

2. ISO/IEC 27001. Information security management systems.

3. W. Stallings. Network Security Essentials.