AL-FARABI KAZAKH NATIONAL UNIVERSITY

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

LEGAL REGULATION OF INFORMATION SECURITY

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

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.

CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

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.

AUTHENTICITY AND NON-REPUDIATION

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.

IDENTITY AND ACCESS IN ICT SYSTEMS

1. Identification	2. Authentication	3. Authorization	4. Accountability
The user presents an identifier, such as a university account name.	The system verifies the claimed identity using a password, security key or another credential.	The system checks what the authenticated user is allowed to do. A lecturer may edit grades only for assigned courses.	The system records actions so that changes can be reviewed later.

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.

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.

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.

CASE DISCUSSION

Scenario

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

Question 1

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

Question 2

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

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.

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.