# 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 6

# PROTECTION OF INFORMATION SYSTEMS AND ELECTRONIC INFORMATION RESOURCES

## LECTURE OBJECTIVE

Explain the goals of protecting information systems and electronic resources and apply legal, organizational and technical measures to a service disruption.

## LECTURE PLAN

1. Protection goals and threats

2. Legal, organizational and technical controls

3. Responsibilities, response and recovery

## PROTECTION GOALS

| Concept or participant | Meaning, duties and application |
|---|---|
| **Confidentiality** | Limit access to restricted electronic resources and prevent unauthorized disclosure. |
| **Integrity and preservation** | Prevent unauthorized changes, deletion and loss. |
| **Authorized access** | Keep resources available to people who have the right to use them. |
| **Continuity** | Reduce disruption to information systems, networks and critical infrastructure. |

Protection addresses both unauthorized conduct and accidental events. A mistaken configuration change can affect the same resource as deliberate interference. Controls therefore need to account for human error, equipment failure and malicious activity. The practical priority depends on the importance of the service and the consequences of losing the information.

## EVENTS THAT COMPROMISE PROTECTION

| Concept or participant | Meaning, duties and application |
|---|---|
| **Access blockage** | An outage or access restriction prevents authorized users from reaching a service or resource. |
| **Modification or copying** | Data is changed or duplicated without permission or through human error. |
| **Loss or destruction** | Resources are deleted, damaged or rendered unrecoverable. |
| **Service disruption** | Failures in software, systems or telecommunications interrupt processing or transmission. |

Blocking, copying, alteration and destruction can occur together. A compromised account may disclose records and change them during the same session. The incident record identifies each effect and the affected resources. This detail helps select containment and recovery measures and supports any later assessment of responsibility.

# LEGAL AND ORGANIZATIONAL MEASURES

| Concept or participant | Meaning, duties and application |
|---|---|
| **Legal measures** | Legislation, standards and agreements set duties, conditions of access and responsibility for breaches. |
| **Organizational measures** | Internal rules define roles, permitted access, procedures for changes and incident escalation. |
| **Physical access** | Entry controls limit access to rooms and facilities where equipment or electronic media are kept. |

Legal measures establish duties and operating conditions. Organizational measures assign people and procedures to fulfil them. Physical entry restrictions protect the places where processing and storage occur. Together these measures determine who can reach an asset, which operations are allowed and how the organization checks whether the rules were followed.

# TECHNICAL MEASURES

**Access control**

Permissions limit access to systems and resources according to assigned roles.

**Event logging**

Records of access and activity support detection, investigation and accountability.

**Protection tools**

Encryption and other security tools protect data according to its classification and operating environment.

**Recovery controls**

Backups and restoration checks support recovery when records are lost or altered.

Access controls prevent some unauthorized operations, while logs help detect and investigate activity that has occurred. Recovery controls address loss or alteration. Cryptographic mechanisms protect information in defined circumstances. The choice of tools follows the information category and system requirements, and their operation depends on configuration and maintenance.

# RESPONSIBILITY FOR PROTECTION

**Electronic information resources**

Owners, holders and users have responsibilities tied to their roles and access.

**Infrastructure**

Owners and holders protect the systems and facilities they operate.

**E-government and critical infrastructure**

The lecture describes additional arrangements for detection, coordination, incident notification and recovery.

**Personal data**

The lecture traces protection duties from receipt of the data through destruction or anonymization.

Protection duties follow the participant’s role and the object involved. The resource owner, system operator and infrastructure provider may be different parties. Their agreements define operational responsibilities, but applicable legal duties also remain relevant. Personal data protection continues through processing and storage until the relevant destruction or anonymization.

# ORGANIZING PROTECTION IN PRACTICE

**Inventory and classification**

Identify resources, systems, owners, dependencies and access restrictions.

**Risk assessment**

Identify credible failure scenarios and assess their consequences for the information and service.

**Control selection**

Assign responsibilities and select measures for prevention, detection and recovery.

**Review**

Test restoration, review permissions and records, and update procedures after changes or incidents.

An inventory identifies what the organization has and who is responsible for it. Classification establishes sensitivity and operational importance. Risk assessment connects threats and weaknesses with potential consequences. Control selection then leads to implementation and review, including checks that permissions remain appropriate and restoration actually works.

# INCIDENT RESPONSE AND RECOVERY

**Detection**

Record the affected service and preserve relevant evidence.

**Containment**

Limit further unauthorized access and prevent the impact from spreading.

**Coordination**

Notify the responsible parties and use the reporting channels applicable to the system.

**Restoration**

Recover affected resources, check their integrity and confirm that the service works.

An incident response includes preserving evidence as well as restoring service. Logs and copies of affected records can explain what happened before recovery changes the environment. After restoration, the organization verifies integrity and availability. It also addresses the cause and any weaknesses that could allow a similar incident to recur.

# CASE DISCUSSION

An account with access to a university registry is misused. Several records are changed, and the registry is temporarily taken offline.

Which controls could have reduced the chance of unauthorized changes?

What evidence and recovery checks are needed before reopening the registry?

**Analysis**

Limit edit access and review privileges. Preserve logs and affected records, verify restored values against a trusted baseline and test the registry. Prevention, detection and verified restoration each address a different part of an incident.

# PREVENTION, DETECTION AND RESTORATION DUTIES

The lecture describes preventing unauthorized access and detecting it promptly when prevention fails. It also identifies minimizing consequences and preventing interference with processing or transmission facilities.

Restoration concerns resources modified or destroyed during an incident. The organization checks recovered data and service operation before closing the response.

Entry controls limit access to buildings and rooms that contain equipment or electronic media. Access procedures identify authorized staff and record visits where required.

Organizational controls also define who grants access, who reviews it and who responds to suspicious activity. Physical access and logical permissions address different ways of reaching the same information.

## CRITICAL INFRASTRUCTURE AND NATIONAL COORDINATION

Owners of e-government and critical infrastructure systems participate in monitoring and incident coordination arrangements described in the lecture. The national centre receives information that supports a wider assessment of the incident.

The source also discusses national backup arrangements and special operating conditions during emergencies. Continuity depends on both local recovery capacity and coordination with external participants.

Protection begins when the system receives electronic resources containing personal data. The lecture follows that duty through storage and processing until destruction or anonymization.

Access reviews, backup controls and transfer records need to reflect where copies of the data exist. Deleting a record from the main application may leave copies in exports or backups governed by their own retention arrangements.

## CONCLUSION

1. Protection includes legal duties, organizational procedures and technical controls.

2. Responsibilities depend on the asset and the party’s role.

3. Prevention, detection and verified restoration each address a different part of an incident.

## SELF-ASSESSMENT QUESTIONS

1. What are the main objectives of protecting information systems and resources?
2. How do legal, organizational and technical protection measures differ?
3. What controls help prevent unauthorized changes to information?
4. What actions support containment and evidence preservation during an incident?
5. How can an organization verify that a system has been successfully restored?

## REFERENCES

1. Lecture 6. Protection of Information Systems and Electronic Information Resources. Course materials.

2. ISO/IEC 27001:2022. Information security management systems.

3. M. E. Whitman and H. J. Mattord. Principles of Information Security.