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 2

PUBLIC INSTITUTIONS AND E-GOVERNMENT

LECTURE 7

STATE BODIES AND ORGANIZATIONS RESPONSIBLE FOR INFORMATION SECURITY

LECTURE OBJECTIVE

Explain how public bodies, infrastructure operators and incident response organizations divide responsibilities for information security in Kazakhstan.

LECTURE PLAN

1. Government policy and critical infrastructure

2. Operational centres and national coordination

3. Service operation, research and investigation

GOVERNMENT AND THE AUTHORIZED BODY

Concept or participant	Meaning, duties and application
Government	Sets national requirements for ICT and information security and adopts the national incident response plan.
Authorized body	Develops requirements, criteria for critical infrastructure and procedures for monitoring and security testing.
Oversight	The authorized body monitors compliance and can issue corrective orders within its competence.

National requirements provide a common basis for different public bodies and infrastructure owners. The authorized body develops procedures and exercises oversight within its competence. Owners implement the requirements in their systems. This division links policy, supervision and day-to-day operation without placing every activity in a single organization.

CRITICAL INFORMATION INFRASTRUCTURE

Concept or participant	Meaning, duties and application
Definition	Facilities are critical when interruption could seriously affect public services, the economy, national security or public safety.
Designation	Classification links a facility's function and potential consequences to additional protection and monitoring arrangements.
Owners	Operators and owners protect their infrastructure and coordinate with the appropriate security bodies.

The criticality of a facility depends on the consequences of interruption. Effects can extend beyond one owner to public safety, public services or the economy. Classification therefore considers the function of the facility and its dependencies. Additional monitoring and coordination arrangements reflect the wider impact that a failure could have.

OPERATIONAL SECURITY CENTRES

Concept or participant	Meaning, duties and application
Monitoring	A security operations centre collects event data and assesses suspicious activity on connected systems.
Coordination	The centre shares incident information with the infrastructure owner and the national coordination centre.
Confidentiality	Information received through monitoring retains its access restrictions.

An operational centre needs reliable event feeds and a clear relationship with the connected owner. It collects and stores information, evaluates threats and communicates findings. Restricted information received through these activities retains protection requirements. Timely notification allows the owner to act while the national centre assesses possible wider effects.

CERT AND NATIONAL COORDINATION

Incident response service

CERT analyses reports, informs affected organizations and prepares guidance for limiting threats.

National coordination centre

Coordinates monitoring between operational centres and consolidates information about significant incidents.

State Technical Service

The lecture assigns it functions in security testing, gateway maintenance and national coordination.

The response service investigates technical causes and prepares recommendations. The national centre consolidates information and coordinates participating operational centres. The State Technical Service performs the functions assigned to it in the source framework. These different roles contribute to detection, analysis and coordinated action when several systems are affected.

E-GOVERNMENT OPERATION AND INTEGRATION

Infrastructure operator

The lecture assigns National Information Technologies JSC responsibility for technical operation and protection of state resources hosted on its infrastructure.

Service integration

An integration function connects public systems and services so they can exchange data.

Local authorities

Support access to public digital services and carry out relevant duties within their territory.

The operator maintains the infrastructure and the services assigned to it. Integration connects systems so they can exchange resources. Local and central authorities also have duties related to access and service provision. An incident affecting a shared platform requires identifying which party can change the infrastructure and which owns the affected records.

RESEARCH AND LAW ENFORCEMENT

Research and standards

Scientific institutions contribute technical expertise, standardization and professional training.

Investigation

Competent law enforcement bodies investigate possible offences according to their jurisdiction.

International cooperation

Response teams can exchange incident information through established channels.

Research institutions contribute standards, technical evaluation and professional training. Law enforcement bodies investigate suspected offences within their jurisdiction. International cooperation can support information exchange and response to events involving other countries. Technical assistance, regulatory oversight and criminal investigation each have their own purpose and authority.

CASE DISCUSSION

An operational centre detects a major outage in a platform shared by several government agencies.

Who restores the service, who coordinates information exchange and who investigates a suspected offence?

Analysis

The owner or operator restores the platform. The operational and national coordination centres share incident information. The competent investigative body handles any suspected offence. System owners remain responsible for their services and work with competent bodies during an incident.

FUNCTIONS OF THE AUTHORIZED BODY

The lecture assigns the authorized body responsibility for developing uniform requirements, critical infrastructure criteria and testing methodologies. It also describes oversight of compliance and coordination of security-related activities.

Other functions include rules for monitoring, information exchange and trusted software arrangements. These functions connect policy requirements to implementation across participating organizations.

An operational centre collects and analyses security events from connected systems. It identifies threats, informs owners and shares information with the national coordination centre.

A response service analyses incidents and recommends measures to remove their causes and conditions. Staff in both functions protect commercial and other restricted information obtained through their work.

NATIONAL COORDINATION AND BACKUP INFRASTRUCTURE

The national coordination centre consolidates information from operational centres and supports joint action across sectors. A wider view helps identify related incidents affecting multiple services.

The lecture also assigns it a role in national backup arrangements for electronic resources. Coordination includes defining the exchange of information and supporting the safe operation of critical systems.

The source describes the State Technical Service maintaining security gateways, testing systems and reviewing security aspects of technical specifications and investment proposals.

Public infrastructure operators maintain services and protect the resources hosted on their infrastructure. Integration functions connect systems while preserving the responsibilities of their owners.

CONCLUSION

1. Government and the authorized body set or develop common requirements.

2. Operations centres, CERT and the national coordination centre have distinct incident functions.

3. System owners remain responsible for their services and work with competent bodies during an incident.

SELF-ASSESSMENT QUESTIONS

1. How do policy development, oversight and operational security functions differ?
2. What responsibilities do system owners retain during an incident?
3. How do operational security centres and national coordination bodies cooperate?
4. Why does critical information infrastructure require particular attention?
5. How does a clear division of competence improve incident handling?

REFERENCES

1. Lecture 7. State Bodies and Organizations Responsible for Information Security. Course materials.

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

3. International Telecommunication Union. Global Cybersecurity Index.