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 2

LEGAL REGULATION OF INFORMATION SECURITY

LECTURE OBJECTIVE

Explain the hierarchy of legal acts in Kazakhstan and relate it to information security oversight, incident coordination and liability.

LECTURE PLAN

1. Privacy protections and the hierarchy of legal acts

2. Monitoring, testing and coordination

3. Civil, administrative and criminal liability

PRIVACY AND PROTECTED INFORMATION

Concept or participant	Meaning, duties and application
Constitutional basis	The lecture uses Article 18 to illustrate constitutional protection of private and family life and confidential communications.
Communications and savings	The lecture identifies correspondence, telephone calls, messages, deposits and savings as protected interests.
Other protected information	State, commercial and banking secrets are governed by distinct legal regimes. Access rules depend on the category of information.

Information about private life, communications and financial affairs may be protected by different provisions. The type of secret or restricted information therefore matters when deciding who may access it. The legal framework also includes duties concerning commercial information, official records and state secrets, each with its own scope.

HIERARCHY OF NORMATIVE LEGAL ACTS

Concept or participant	Meaning, duties and application
Constitution	The Constitution has the highest legal force in the hierarchy described in the lecture.
Legislative acts	Constitutional amendments and constitutional laws precede codes, consolidated laws and ordinary laws.
National subordinate acts	The lecture places normative parliamentary resolutions before presidential decrees, government resolutions and central agency orders.
Departmental and local acts	Departmental orders and normative acts of local bodies appear at lower levels. Higher-ranking provisions prevail in a conflict.

A lower-level rule is interpreted within the authority granted by higher-level acts. Internal procedures implement applicable duties within an organization. They also need to identify responsible staff and provide usable instructions. The legal hierarchy becomes important when an operational rule conflicts with a superior provision or exceeds the issuing body’s powers.

LEGAL INSTRUMENTS AND THEIR SCOPE

Concept or participant	Meaning, duties and application
Civil, criminal and administrative codes	These address civil relationships, offences, liability and associated procedures.
Sector laws	The source discusses legislation on informatization, personal data, state secrets, communications and access to information.
Uniform ICT and security requirements	Government Resolution No. 832 of 20 December 2016 is an example of detailed technical and organizational regulation.

The regulatory system combines general rules with sector-specific requirements. Civil law addresses relationships between parties, while criminal and administrative provisions define particular violations and consequences. Technical requirements translate legal duties into procedures for operating systems. Their application depends on the system, information category and organization involved.

DEVELOPMENT OF THE LEGAL FRAMEWORK

1997–1998

The 1997 Criminal Code addressed unauthorized access. A 1998 government resolution addressed coordination of national information infrastructure and security.

2003 and 2007

Successive informatization laws developed the framework for electronic resources, information systems and their use.

2015–2016

A further informatization law and implementing measures addressed electronic government, security testing and critical infrastructure.

The historical development in the source shows an expanding role for electronic resources as assets and for digital services in public administration. Successive legislation differentiated public and restricted resources and established duties for owners, holders and users. The growth of e-government also increased the need for common testing and monitoring arrangements.

MONITORING AND SECURITY TESTING

Operational monitoring

Monitoring of e-government systems helps identify security events and notify system owners so they can respond.

Pre-deployment testing

The lecture describes reviewing source code and security settings, examining network and server equipment, and conducting load tests during trial operation.

Critical infrastructure

Classification determines which facilities fall under special protection and monitoring arrangements.

Security testing can identify defects before operation, while monitoring can identify events after deployment. Testing includes application logic, configuration, network and server equipment, and performance under load. Results support corrections to security and fault tolerance. Retesting and operational records help establish whether the identified problem was addressed.

INCIDENT COORDINATION AND COOPERATION

System owners and sector bodies

Owners address issues in their systems. Public bodies act within their respective areas of responsibility.

KZ-CERT

Kazakhstan’s computer incident response service assists organizations and users with computer security incidents.

Cyber Shield of Kazakhstan

The national cybersecurity concept provides context for incident response, protection of critical infrastructure and cooperation with international response teams.

Information exchange between owners and response bodies helps establish whether an event affects one organization or several. A response service can analyse technical causes and provide recommendations. Owners still need to implement measures in their environment and communicate the impact on their services. International cooperation can support incidents involving external infrastructure.

LIABILITY FOR VIOLATIONS

Civil liability

A violation can create a dispute over contractual duties, losses or compensation.

Administrative liability

Administrative provisions can apply to failures to follow security or personal data protection requirements.

Criminal liability

Conduct involving information resources or networks may constitute a criminal offence when the statutory elements are met.

Liability requires an applicable rule and evidence of the relevant facts. The organization’s records may show whether required measures were taken, whether an actor had authority, and how an event caused harm. A technical incident report can support the assessment, but the legal procedure determines the effect of that evidence.

CASE DISCUSSION

A government portal experiences a technical failure and exposes restricted records. A monitoring centre alerts the system owner.

Which questions concern operational response, and which concern legal liability?

Where would the owner look for applicable technical and organizational requirements?

Analysis

Contain the exposure, preserve evidence and coordinate restoration. The legal assessment separately establishes duties and possible liability. The facts and applicable provisions determine the type of legal liability.

UNIFORM REQUIREMENTS ACROSS THE SYSTEM LIFECYCLE

The lecture presents the Uniform Requirements as a combination of legal and technical provisions affecting systems, resources, software and equipment. Their application extends across development, testing and operation.

A project therefore includes security requirements in its technical specification. Testing checks whether the implementation meets those requirements. Operational monitoring checks how the deployed service behaves over time.

The source describes reviewing source code, checking security settings, examining network and server equipment, and conducting load tests. These checks address different failure mechanisms and produce complementary findings.

A source code review may reveal a defect in application logic. A configuration review may reveal excessive permissions. Load testing may identify capacity limits that affect availability during peak demand.

PROTECTION OF STATE SECRETS AND PERSONAL DATA

Different information categories have different protection regimes. The lecture describes special-purpose networks and cryptographic protection for state secrets, including physical separation from public Internet infrastructure.

For personal data, the source discusses collection and processing grounds, storage conditions, destruction and cross-border transfer. The purpose of processing and the applicable exceptions shape the duties of the parties.

To assess a possible violation, identify the applicable provision and the party to whom it applies. Then compare the required action with the records showing what actually happened.

Relevant material can include testing results, system configurations, access records and incident notifications. A technical failure alone does not establish every element needed for a particular form of liability.

CONCLUSION

1. The hierarchy of legal acts determines which provisions prevail when rules conflict.

2. Monitoring, security testing and incident response serve different purposes.

3. The facts and applicable provisions determine the type of legal liability.

SELF-ASSESSMENT QUESTIONS

1. What is the purpose of legal regulation in information security?
2. How does the hierarchy of legal acts affect the application of security requirements?
3. How do organizations translate legal requirements into internal procedures?
4. What are the differences between monitoring, security testing and incident coordination?
5. What factors determine the legal consequences of a security violation?

REFERENCES

1. Lecture 2. Legal Regulation of Information Security. Course materials.

2. Government Resolution No. 832 of 20 December 2016. Uniform Requirements for ICT and Information Security.

3. Republic of Kazakhstan. Law On Legal Acts.