Lecture-1. The concept of information security

Lecture Objective:

To study the essence of information security, its principles, objectives, and legal framework in the Republic of Kazakhstan. To familiarize students with key concepts such as confidentiality, integrity, and availability, as well as the fundamentals of state policy in the field of information protection.

Main Questions:

- Definition and importance of information security
- State regulation of informatization and security
- Principles of information security in Kazakhstan
- Main state tasks in informatization management
- Classical model: confidentiality, integrity, availability
- Additional properties: authenticity, non-repudiation
- Identification and authentication in ICT systems
- Cybersecurity as a subsection of information security

Information is both a valuable resource and an asset of both a particular person and an organization and the state as a whole. The development of infocommunication means causes not only the possibility of a constant increase in the volume of collection, processing, storage and transmission of information, but also an ever-increasing need to ensure the protection of such information and to organize such a process of its use, which eliminates or minimizes its losses, and the process of using it information remains continuous. And like any complex and multi-component process, it strives for automation - i.e. the use of information and communication technology tools to optimize the creation, search, collection, accumulation, storage, processing, receipt, use, transformation, display, distribution and provision of information.

Thus, information security implies the protection of information and the work of the user / organization / state with it from intentional or accidental (negligence, negligence, etc.) actions or inaction that lead or may lead to damage to both its owners and owners, as well as and users of it, as well as other persons involved in the process of collecting, processing, transferring and storing information. It is obvious that the preventive aspect will play a large role in the protection of information - i.e. prevention of information security violations rather than elimination of the consequences thereof, because the consequences/damage may not always be immediately assessed in full.

In this regard, the state pays special attention to the regulation of public relations in the field of informatization, the purpose of which is the formation and development of information and communication infrastructure for information support of social and economic development and competitiveness of the Republic of Kazakhstan.

State regulation of processes in the field of informatization, incl. in the field of information security is based on the following principles:

1) legality - i.e. strict observance of the rules of conduct established in the state by all;
2) observance of the rights, freedoms and legitimate interests of individuals, as well as the rights and legitimate interests of legal entities - i.e. prevention of violations of the rights of the above persons;
3) equality of the rights of individuals and legal entities to participate in activities in the field of informatization and use its results - i.e. the same regulatory approach to all subjects and persons;

4) ensuring free access to electronic information resources containing information about the activities of state bodies (presumption of openness), and their mandatory provision, except for electronic information resources, access to which is limited in accordance with the laws of the Republic of Kazakhstan - i.e. freedom to receive information with restrictions established by law;
5) the timeliness of provision, objectivity, completeness and reliability of electronic information resources, in respect of which the laws of the Republic of Kazakhstan establish the mandatory nature of their public distribution or provision by state bodies - i.e. publicity of state power;
6) freedom of search, formation and transfer of any electronic information resources, access to which is not limited in accordance with the laws of the Republic of Kazakhstan - i.e. freedom to receive and transmit information;
7) ensuring the security of the individual, society and the state when using information and communication technologies (ICT) - i.e. protection of individuals, legal entities and the state in the process of use (ICT);
8) creating conditions for the development of the information and communication technologies industry and fair competition - i.e. freedom of choice;
9) ensuring centralized management of objects of informatization of "electronic government" - i.e. unified management by the state by "electronic government";
10) implementation of informatization activities on the territory of the Republic of Kazakhstan on the basis of uniform standards that ensure the reliability and manageability of informatization objects - i.e. unification and unitarization of applicable standards and requirements.

In this regard, the state sets itself the following tasks in the management of informatization processes:

1) formation and development of the information society;
2) ensuring the implementation and support of the administrative reform of state bodies;
3) development of "electronic government" and "electronic akimat";
4) increasing digital literacy;
5) providing participants in the educational process with conditions for access to electronic information resources of e-learning;
6) providing conditions for the development and implementation of modern information and communication technologies in production processes;
7) assistance in the formation and development of the domestic industry of information and communication technologies;
8) formation and implementation of a unified scientific, technical, industrial and innovative policy in the field of informatization;
9) formation, development and protection of state electronic information resources, information systems and telecommunications networks, ensuring their interaction in a single information space;
10) monitoring of ensuring information security of state bodies, individuals and legal entities;
11) prevention and prompt response to information security incidents, including in emergency situations of a social, natural and man-made nature, the introduction of a state of emergency or martial law;
12) creation of conditions for attracting investments in the field of information and communication technologies on a systematic basis;
13) improvement of the legislation of the Republic of Kazakhstan in the field of informatization;

14) participation in international cooperation in the field of informatization;

15) creation of conditions for international information exchange and access to information.

Obviously, even in the presence of public information and obligations to disclose it, the very process of its disclosure, in terms of reliability and immutability, will also come down to protecting this information.

Note: Detailed implementation of the principles and tasks of state regulation and management will be considered in subsequent lecture materials and seminars.

As you can see, the beginning of the process of state regulation of information security issues begins with the establishment of relevant provisions and rules in the legislation - both describing procedures and processes in relation to information security, and establishing responsibility for information security violations, as well as procedures for investigating and punishing those responsible.

Information security *in accordance with the legislation of the Republic of Kazakhstan - the state of protection of electronic information resources, information systems and information and communication infrastructure from external and internal threats.* But no state of security is possible as a result of "doing nothing" - inaction, i.e. this is primarily the result of vigorous activity, and not only on the part of the state. In this regard, in our opinion, the most capacious concept of information security is given by the domestic author Chernov I. - "this is the process of ensuring the confidentiality, integrity and availability of information"1. And then it is quite logical that the task of information security by this author is "an activity aimed at preventing unauthorized and unintentional impact on protected information, as well as preventing unauthorized and unintentional leakage of information through any possible channels." As we can see, the prevention of information security violations (information security) once again comes to the fore, although in our opinion - the issues of investigation, responsibility and punishment cannot be excluded from information security either - the threat of prosecution stimulates not only the creation and development of information security systems designed to preventively protect information (for example, Kaspersky Internet Security, etc.), but it can also "cool" some "hot heads" from committing illegal acts in the future.

Legislation, along with the concept of information security, also appeals to the concept of ***information protection and cybersecurity***, which means the state of protection of information in electronic form and the environment for its processing, storage, transmission (electronic information resources, information systems and information and communication infrastructure) from external and internal threats, then there is information security in the field of informatization.

What is the protection of information and electronic information resources and why is it needed? Protection of information or electronic information resources and information systems is a set of physical, technical, software, cryptographic and administrative measures aimed at ensuring information security. Those. information security is only one of the parts / sections of information security. In the future, we will consider these and other components of information security in more detail.

The classical model of information security is based on the provision of three attributes that are significant for information security:

1. Privacy
2. Integrity
3. Availability.

Confidentiality of information means that only a strictly limited circle of persons, determined by its owner or owner, can get acquainted with it. If information is accessed by an unauthorized person, unauthorized access or confidentiality occurs, along with the fact that copying or modification of information may occur, such information itself becomes compromised in its essence, and then the owners / owners have questions about its changes, which is not always possible . In subsequent lectures, we will consider the statutory liability for such acts.

For some types of information protected by law or by the owner or owner, confidentiality is one of the most important attributes (official information, various types of secrets protected by law - commercial, medical, banking, etc., personal data of limited access, for example, information about customers bank, creditors, tax data, information from medical institutions about the health status of patients, etc.).

Integrity of information - the ability of information (data) to be preserved in an undistorted form. Unlawful or unforeseen or unauthorized changes to information by the owner or owner (as a result of a user/administrator's mistake or a deliberate action by an unauthorized person) lead to a violation of the integrity of information. Particularly important is the integrity of data related to the operation of critical information and communication infrastructure facilities (for example, continuously operating systems 24 hours a day - automated air traffic control systems, electricity and power supply, and so on).

The availability of information is determined by the ability of the information system to provide timely, unhindered access to information to subjects with the appropriate authority - i.e. those to whom the owner or +owner of the information has authorized such access. Destroying or blocking information (whether by mistake or intentional action) results in a loss of availability. Sometimes the loss of accessibility is also possible as a result of modification of the information itself or information about the conditions for accessing it - i.e. destroying the original information and replacing it with another one - unreliable, compromised, etc.

Accessibility is an important attribute for the functioning of information systems focused on customer service through the provision of information and communication services (information systems for the sale of railway and air tickets, banking services, distribution of products by Internet resources and electronic media on the Internet, etc.). The situation when an authorized user cannot access certain services (most often networked) or their results is called a denial of service.

In connection with the development of communication (network technologies), two more properties of information security are additionally distinguished, related to the identity of a person managing or using an information system or an electronic information resource using a network remotely:

- authenticity
- appellability.

Authenticity - the ability to reliably identify the author of a legally significant action in a network with information or a message in the field of information and communication services, for example, in e-commerce, when a digital signature or other authentication method is used - via SMS, biometric identifiers, etc.

Appealability (non-repudiation) is the possibility, in case of refusal of authorship, to prove that the author of actions with information in an information system or in an Internet resource is precisely this user and no one else by registering the actions performed by him.

A few more concepts in the field of information security:

Authentication (authentication) - verification of belonging to the access subject of the identifier presented to them and confirmation of its authenticity.

Identification is the assignment to subjects of access to an information system or an electronic resource of a personal identifier that provides authentication and determination of the powers of the subject when he is admitted to the information system, control of powers in the course of a session and registration of his actions.

Identification and authentication is the basis of modern software and hardware and hardware and software information security, since any ICT services and services are mainly designed to serve the subjects-users of ICT services.

However, we repeat - all of the above is typical for cybersecurity, while cybersecurity is just one of the sections of information security in relation to information in electronic form.

Thus, in our opinion, information security in the legal aspect is the procedure established by law for the circulation of information and the functioning of related infrastructure in society and in the state through information systems, info-communication networks and infrastructure, as well as the established responsibility for its violation.

Let us consider what the legal system of information security regulation is and what legal acts regulate information security in the Republic of Kazakhstan.

Control Questions:

1. Define the term *information security*.
2. List and explain the main principles of state regulation in the field of informatization.
3. What are the three key attributes of information security?
4. What is the difference between information protection and information security?
5. Explain the concepts of authenticity and non-repudiation.
6. What is the purpose of identification and authentication in ICT systems?
7. How does the Republic of Kazakhstan ensure information security at the state level?
8. What is cybersecurity, and how is it related to information security?

Recommended Literature:

1. Chernov I. *Information Security: Concepts and Mechanisms.*
2. Legislation of the Republic of Kazakhstan on Informatization and Cybersecurity.
3. ISO/IEC 27001: *Information Security Management Systems Requirements.*
4. Stallings, W. *Network Security Essentials.*
5. Peltier, T. *Information Security Policies and Procedures.*
6. Concept of cybersecurity ("Cybershield of Kazakhstan")
7. Казанцев Виталий Витальевич, Конспект лекций по учебному модулю «Правовое регулирование информационной безопасности в Республике Казахстан», Алматы, 2019
8. Azamatova A.B. , Balpanova N.A., "Kazakhstan’s cyber shield" – a priority vector of implementation of the national security of the republic of Kazakhstan», BULLETIN Abay Kazakh National Pedagogical University, Almaty, 2017
9. Сабитов Д. Информационная безопасность Казахстана: защита данных и смыслов. - Астана, 2015