Lecture-3. Legally significant actions in information systems and in info-communication networks

Lecture Objective:

To examine the concept and characteristics of legally significant actions performed within information systems and info-communication networks. The lecture aims to define the legal status of electronic transactions, explore mechanisms for authentication and digital signatures, and analyze the legal implications of actions performed in electronic environments under Kazakhstani and international law.

Main Subtopics:

- Definition and legal nature of legally significant actions
- Legal recognition of electronic documents and digital signatures
- Requirements for identification and authentication of users in information systems
- Procedures for verifying authorship and ensuring non-repudiation
- Legal consequences of electronic actions in e-government systems
- Electronic contracts and transactions in civil and commercial law
- Regulation of data exchange in info-communication networks
- Evidence and liability in cases of electronic disputes
- International legal standards for electronic interactions (UNCITRAL Model Law, ISO/IEC 27001)

The use of information systems and Internet resources is usually aimed at obtaining or transmitting information, and information incl. and as a result of the provision of services - commercial, public (through the e-government portal), or the receipt / transfer of goods (online stores, etc.). Those. in any case, before accessing an information system or an Internet resource, the user enters into a number of transactions - with a telecom operator for the provision of communication services, with the owner / owner of the resource - a user agreement, a specific application / order for a service, etc. Those. the user and his counterparty reach an agreement on a specific issue(s) of working with information.

In accordance with the law, transactions are recognized as actions of citizens and legal entities aimed at establishing, changing or terminating civil rights and obligations. Transactions can be unilateral and two- or multilateral (contracts). A unilateral transaction is considered to be a transaction, for the conclusion of which, in accordance with the legislation or agreement of the parties, it is necessary and sufficient to express the will of one party. To conclude a contract, it is necessary to express the agreed will of two parties (bilateral transaction) or three or more parties (multilateral transaction).

Transactions are made orally or in writing (simple or notarial). The written form of the transaction is made on paper or in electronic form. A transaction made in writing must be signed by the parties or their representatives. When making a transaction, it is allowed to use means of facsimile copying of a signature, an electronic digital signature (EDS), if this does not contradict the law or the requirement of one of the participants in the transaction.

Bilateral transactions can be made through the exchange of documents, each of which is signed by the party from which it originates. Unless otherwise established by law or agreement of the parties, the exchange of letters, telegrams, telephone messages, teletype messages, faxes, electronic documents with EDS, electronic messages or other documents defining the subjects and the content of their will is equated to the conclusion of a transaction in writing, unless otherwise provided by law or agreement of the parties.

Thus, in relation to information systems and Internet resources, it is obvious that transactions in them can be concluded both by directly signing them by the parties with their EDS, and by exchanging electronic documents with EDS or electronic messages. And here, in relation to the field of information security, the question of authentication and identification of the parties arises. If in the case of an EDS, everything is relatively clear - confirmation of the compliance of the EDS key is given by a third party - a certification center, then in the case of the exchange of electronic messages, difficulties arise. To understand the issue, we note two main aspects, without which the deal will not be concluded:

- determination/identification of the party to the transaction - i.e. identification of the sender/recipient of such a message.
- accessibility/readability/understanding of the content of such a message.

How is it implemented? So, for example, in accordance with the law, the provision by the owner or owner of a public electronic information resource of a service for posting information by a user is carried out on the basis of an agreement concluded in writing (including electronic), with identification on the e-government portal or through the use of a registered on the public information electronic resource of the user's cellular subscriber number by sending a short text message containing a one-time password to conclude an agreement. Those. instead of an EDS, as an option, a registered cellular subscriber number is used as an identifier. Those. the agreement itself, an application for sending a short SMS, receiving a password via SMS and entering it during identification - in fact, is the conclusion of a transaction between the owner of the EIR and the person for whom the cellular number is registered.

Why is it important to understand the conclusion of a transaction - a user agreement, etc.? Because in the absence of a concluded transaction, because it is recognized as invalid / void, we get a situation that the user has accessed and used information without the permission of the owner / owner of the information system, EIR, etc. – i.e. in fact, unauthorized access to information is obtained - i.e. information security breach. At the same time, it is important to understand that, as a rule, a transaction can be invalidated after such access - i.e. in any case, information in the information system, etc. will already be compromised. An invalid transaction does not entail legal consequences, except for those related to its invalidity, and is invalid from the moment it was made.

The grounds for the invalidity of the transaction are:

1. The transaction was made without obtaining the necessary permission or after the expiration of the permission.
2. A transaction that pursues the goals of unfair competition or violates the requirements of business ethics.
3. The transaction is made by a person under the age of fourteen (minor), (there are exceptions in the legislation in this case).
4. A transaction made by a minor who has reached the age of fourteen, without the consent of his legal representatives, except for transactions that he, by law, has the right to make independently.
5. The transaction was made by a person recognized as incapable due to mental illness or dementia.
6. A transaction made by a citizen, although capable, but at the time of its completion in such a state that he could not understand the meaning of his actions or manage them.
7. The transaction was made as a result of a delusion of significant importance. Of significant importance is the misconception about the nature of the transaction, the identity or such qualities of its subject, which significantly reduce the possibility of its intended use. A

mistake in motives can serve as a basis for the invalidity of a transaction only if such a motive is included in its content as a suspensive or resolutive condition.

8. The transaction was made under the influence of deception, violence, threats, as well as a transaction that a person was forced to make due to a combination of difficult circumstances on extremely unfavorable conditions for himself, which the other party took advantage of (enslaved transaction).
9. A transaction made as a result of a malicious agreement between a representative of one party and another party.

   Etc.

It should be noted that the mechanism for invalidating transactions is a judicial procedure. However, there are a number of grounds when a transaction is void - i.e. there is no need to go to court. For example, non-compliance with the written form of a transaction, as well as the exchange of electronic messages without complying with both of the above requirements for them, makes such a transaction void from the very moment of its conclusion, and all user actions on it in an information system or Internet resource can be regarded as an information security violation.

Thus, IS violation is not only a technical aspect of information protection, but also legal support for the process of working with it - from the legal registration of registration and login processes to obtaining the results of services or posting / deleting information. That is why, even in the absence of facts of IS penetration/violation at the technical level, if the agreement is canceled/recognised as invalid, the fact of IS violation on a global level and compromise of information will take place.

In this regard, we can conclude that the organization of information security includes not only organizational, and even more so technical aspects, but also legal ones, and not only in terms of regulating exclusively access procedures, but also the entire process of working with information. That is why the study of the legal regulation of information security is important for non-specialists in the field of jurisprudence.

Control Questions:

1. What are legally significant actions in the context of information systems?
2. How does the Republic of Kazakhstan legally recognize electronic documents and digital signatures?
3. What is the role of identification and authentication in ensuring legal validity?
4. Explain the concept of non-repudiation and its importance in electronic communications.
5. What legal consequences arise from actions performed in e-government systems?
6. How are electronic contracts and transactions regulated in Kazakhstan?
7. What are the main principles of liability in cases involving electronic information?
8. Which international documents establish standards for electronic legal acts?

Recommended Literature:

1. Law of the Republic of Kazakhstan “On Electronic Document and Electronic Digital Signature.”
2. Civil Code of the Republic of Kazakhstan (sections on electronic transactions).
3. Law of the Republic of Kazakhstan “On Informatization.”
4. UNCITRAL Model Law on Electronic Commerce (1996).
5. ISO/IEC 27001: Information Security Management Systems Requirements.
6. Peltier, T. *Information Security Policies and Procedures.*
7. Stallings, W. *Network Security Essentials.*
8. Chernov I. *Information Security: Concepts and Mechanisms.*