THE ROLE OF INFORMATION SECURITY IN SOCIETY

Doszhanov B.A.[1], Almenaeva R.U.[2], Nurtasova A.S.[3]

[1]Doszhanov Baiyanali Amantayevich – candidate of pedagogical sciences, associate professor,
DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES;
[2]Almenaeva Raihan Umirzakovna – master of science, senior lecturer,
DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES;
[3]Nurtasova Aliya Sabitovna - master student,
DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES,
KORKYT ATA KYZYLORDA STATE UNIVERSITY,
KYZYLORDA, REPUBLIC OF KAZAKHSTAN

Abstract: *in order to ensure the security of the information space concept for the country, adopted at the state level. This article discusses this concept for the analysis of technical and socio-political aspects of information security. In addition, the issues of information security, are characterized by the ability of cryptographic methods.*

Keywords: *information security, data protection and cryptographic techniques.*

In today's society it is impossible to grow and develop without using information systems which helps to receive, edit, save and offer the data. Modern information technologies generate not only new issues on providing information security, but also it requires a consideration of new ways of solving them.

In the Addressby the President N.A. Nazarbayev from 17th January 2014 called «The Kazakhstan Way: One goal, One Interest and One Future» he says: «The state must stimulate development of transit potential in sphere of information technologies. We must ensure that by 2030 at least 2-3% of global information flows through Kazakhstan. This figure must double by 2050» [1]. On this basis, in order to transfer global information, there is a high importance of providing security.

«The Concept of Information Security of the Republic of Kazakhstan until 2016» was approved by №174 Decree of the President of the Republic of Kazakhstan on November 14, 2011.The main purposes of this Concept are: to find out the interest of the state and society in the information sphere; to improve the regulatory legal acts and the content of public service for the protection from internal and external threats; to analyze the current situation related to information security; to ensure the integrity of the formation and implementation of the principles of methodological framework which regulates this sphere. In the Concept there were identified the main objectives and priorities given to individual man in order to provide the state and society security. Information security of the country is viewed from two inter-related perspectives: technological and socio-political. The technological aspect involves the protection of national information assets, information systems, information and telecommunication infrastructure from unauthorized access, use, disclosure, interruption, modification, reading, verification, data recording or destruction to ensure the integrity, confidentiality and availability of information. The socio-political aspect is the protection of the national information environment and mass media from purposeful negative information and organizational impact that is capable of causing damage to the national interests of the Republic of Kazakhstan [2].

There are 3 important statuses of information security. They are: availability (optimal), integrity, and confidentiality.

Availability (optimal) is the option that allows user to get the necessary information without any obstacles in a few minutes.

Integrity is the assurance that the information has not been altered and truly represents what is intended.It is the protection by the automated systems when someone accidentally or intentionally wants to change the information.

Confidentialityis the option that restricts user from getting the information, i.e. provides protection against unauthorized access or reading.

The current situation related to information security shows the problems as following:

- lack of qualified professionals in the sphere of information security leads to the inability to protect the information from any external threats properly;
- imperfection or frequent destruction of information security systems of very important informatization objects;
- low level of creation, implementation and use of modern information and communication technologies that does not meet the needs of society;
- dependenceof our country on the import of information technology, informatization, information securitytools;
- increase of information attakcs among the world’s leading states, and their aspiration for an excessive influence in the information space;
- inconsistent policy of some states in the sphere of globalinformation analysis;

- development of information manipulation technologies;
- opportunity of influencing provocative information that harms national interest of the country on a public conscience and state institutes;
- unreliable and deliberately distorted information dissemination in order to harm the public interest;
- transparency of the information space, etc [3].

These problems shows the need to pay a special attention to information security not only important state structures, but every social and economic institutions of our country.

One of the main problems that require a solution is a sufficient quantity of professionals in the sphere of information security. Today, in the era of modern information society, it is very crucial to the information technology specialist to learn the science of cryptology, that deals with the problems of protecting the information. Especiallycryptography which deals withthe mathematicalmethods of analyzingthe information andcryptanalysis which helps to decode the information without secret key.

Knowing symmetric cryptosystems such as data encryption and decryption by exchanging places using only one key, to place one or more alphabet, block cipher, additive stream encryption; and assymetric crypto-systems such as El-Gamal, Rivest-Shamir-Eydelman, Merkle-Hellman and Chor-Rivest using one key for encryption,and the second for decryption will improve the quality of information security service.

Cryptographic methods of information protection in automated systems do not only protect the information processed in computer and stored in different storage devices, as well as it is necessary to ensure the completeness of the information transmitted through the channels of network connection [4]. In other words, the use of cryptographic methods gives an opportunity to ensure accuracy of information when sending secret information through communication channels and keeping it in transference devices in encrypted form.

References

1. *Nazarbayev N.A.* Address by the President from 17th January 2014 called «The Kazakhstan Way: One goal, One Interest and One Future».
2. «The Concept of Information Security of the Republic of Kazakhstan until 2016» was approved by № 174. Decree of the President of the Republic of Kazakhstan on November 14, 2011.
3. *Tulbasova B.K., Omarova S.A., Unaibayeva R.K.* Information security and protection of the information. Training and methodology complex. Almaty: Nur-Print, 2012. 115 p.
4. *Siranova A.S.* Cryptographic methods of protecting information in computer networks: master’s thesis prepared for the academic degree of master of science. Kyzylorda: KSU, 2014. 18 p.