THE ROLE OF STENOGRAPHY IN INFORMATION PROTECTION

Mokhigul Majidova
Master's Student, Human Resources Management, Samarkand State University.
Graduate student of the Department of Digital Economy

Ziyovuddin Bakayev
PhD, Faculty of Human Resources Management, Samarkand State University.
Graduate student of the Department of Digital Economy

Annotation
In this article, the problems that arise in the protection of information and the modern progress in the field of global computer networks and multimedia have led to the creation of new methods designed to ensure the safety of data transmission in telecommunication channels. The importance and scope of these methods in the protection of information are described.

Keywords: shorthand, cryptographic methods, container-file, encryption devices, encryption devices.

The problem of reliable protection of information from unauthorized access has existed for a long time and has not been solved until now. Methods of hiding secret messages have been known since ancient times, this field of human activity is called shorthand. This word comes from the Greek words Steganos (secret, secret) and Graphy (writing) and means "mysterious writing". Shorthand techniques probably predated writing (originally using syllabification and punctuation). As we mentioned above, in addition to coding and cryptographic methods, steganographic algorithms are also used to protect information. Stenography has a distinct difference from cryptography. That is, its purpose is to hide the existence of a secret message. Both of these methods can be combined and, as a result, can be used to increase the effectiveness of information protection 20 (for example, for the transmission of cryptographic keys).

Computer technology gave a new impetus to the development and improvement of shorthand. As a result, a new direction in the field of information protection - computer shorthand appeared. Modern progress in the field of global computer networks and multimedia has led to the creation of new methods designed to ensure the security of data transmission in telecommunication channels. These methods make it possible to hide messages in computer files (containers) using the natural ambiguity of encryption devices and the abundance of analog video or audio signals. At the same time, unlike cryptography, these methods hide the fact of information transfer. K. Shannon created a general theory of secret writing, which is the basis of shorthand as a science. There are two main types of files in modern computer

steganography: a message-file, which is intended to be hidden, and a container-file, which can be used to hide a message.
There are two types of containers: container-original (or "empty" container) - this container does not store hidden information; container-result (or "filled" container) - this container stores hidden information. A key is a secret element that determines the order in which a message is inserted into a container. The analysis of the development trend of computer shorthand shows that interest in the development of computer shorthand methods is growing in recent years. In particular, it is known that the urgency of the problem of information security is constantly increasing and the search for new methods of information protection is encouraged. On the other hand, the rapid development of information and communication technologies provides opportunities to introduce new methods of protecting this information, and, of course, a powerful catalyst for this process is the very strong development of the Internet computer network.
Currently, the most widely used methods of information protection are cryptographic methods. However, there are many unsolved problems related to the destructive effect of information weapons such as computer viruses, "logic bombs" on this path. On the other hand, the problem of key distribution in the use of cryptographic methods is still not fully resolved today. The combination of computer steganography and cryptography would be a good way to get out of the situation, because in this case it is possible to eliminate the weak points of information protection methods. Thus, computer shorthand is currently considered one of the main technologies for information security.
The main conditions of modern computer shorthand are as follows: - hiding methods should ensure the authentication and integrity of the file; 21 - it is assumed that the steganography methods used by malicious persons are fully known; - security of the methods is based on the storage of the main properties of the open transfer file with shorthand substitutions and some information - a key - unknown to other persons; - if malicious persons know the time of opening the message, the process of extracting the secret message itself should be considered as a complex calculation problem.
The analysis of information sources of the Internet computer network made it possible to come to the following conclusion, that is, currently, stenographic systems are actively used to solve the following main issues: − protection of confidential information from unauthorized access; - overcome monitoring and management systems of network reserves; - software masking; - protection of copyright in some types of intellectual property. From a security policy perspective, the following sample password requirements can be recommended:
• the password should not be less than 8 characters;
• the password must consist of at least one number and one letter;
• the new password must differ from the previous one by at least 3 characters;
• the password should not overlap with the user ID;

• the password should not be the same as a meaningful word in any language;
• one password should not be used for more than 3 months;
• the password should not consist of the user's last name, first name, first name;
• do not use personal information such as phone number, passport or other document number, car number, time of birth as a password;
•passwords for different systems and services should be different.

In addition, in some systems (for example, when opening an e-mail on mail.ru), during the registration period, if the user forgets the password, the system may choose one of the questions from the list of questions asked in order to restore the password or give the user another password, and it is required to answer. But most users enter the same questions and answers during registration. For example, from the list of questions, "your favorite movie?" and write the name of the movie "Puaro" or similar. Someone who wants to get your password can try to change your password by entering your login and then entering the system through "forgot password". Therefore, it is recommended to use completely new questions and answers during registration

References

1. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2020.
2. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2021 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy.