Steganography

The principle of steganographic methods of information protection is that a violator cannot distinguish meaningful information in the stream of data circulating in the system. Therefore, in this case no issue on possible access to protected information exists at all, because it is absolutely unclear what data should be distinguish as meaningful.

It is generally agreed that the basic requirements for steganographic systems are as follows:

- steganographic methods must ensure authenticity and integrity of files;
- an enemy possesses complete knowledge of steganographic methods;
- steganographic methods must retain principal properties of a file transmitted in clear mode (a stegocontainer) when a confidential message and certain service data unknown to the enemy, for example a key, are entered into such file;
- if an enemy knows about transmission of a certain hidden message, an extraction of the confidential message out of the stegocontainer must represent a complex computational problem.

There are several ways the steganography can be used. They differ principally by the type of containers – those files or messages in which confidential information is built. Graphic and sound containers are traditionally used. Their inherent redundancy allows an additional informational component to be included without detection of its masking container. Considering the fact that current information and telecommunication technologies are digital, the most effective approach seems to be the one that uses the least significant bits of digitized images or acoustic signals as components carrying useful information.

In general steganographic methods can be divided into two groups. The first group includes methods that use special properties of computer data formats, for example methods of information hiding in unusable disk space, and methods of special formatting of text files. In particular, special formatting methods can be implemented by using a known shifting of words, sentences and paragraphs, applying various styles in text processors, such as Microsoft Word, selecting certain positions in a text to insert a hidden message, using special fields that are not displayed on the screen. In addition, more complex methods are also known that are based on creation of a meaning-bearing text for the transmitted confidential message, in order to hide the actual message by certain rules. Also, a fairly frequently used method of separation between stegocontainer transmission and appropriate service data transmission should be mentioned.

The second group of steganographic methods includes those methods based on the use of redundancy of audio and video files. As it can be readily understood, the least significant bits of the most common multimedia formats are the least informative and, therefore, can be used to transmit additional information without affecting their perception by a man.

An analysis of existing methods for hidden message integration into container files showed that the means implementing steganographic methods of information protection, available on the market, have additional weaknesses permitting to reveal availability of the embedded message. It may be said in this connection that such products implement a principle of protection against an honest man that in any case would not be interested in the secrets of others by virtue of his decency. Moreover, the use of such steganographic systems puts a potential enemy in a privileged position permitting him to develop methods in advance to detect transmission of stegocontainers and recover hidden messages from them.

Our company offers both finished systems and development of an exclusive method for integration of private or confidential messages into public files for the convenience of a specific customer. Based on deeply developed theoretical grounds and using experience of the best domestic and foreign designs, our Company offers individual technical solutions for every customer. Original features of steganographic algorithms provide a possibility of making the customer's confidential files reliably hidden from foreign eyes.

At the present time, a combination of different protection methods is the main trend in information protection, which is conditioned by many unsolved problems associated with destructive software effects, such as computer viruses and logical bombs. Combination of both computer steganography and cryptography methods just helps to find solutions to such problems. As a result, many weaknesses of known data protection methods can be eliminated and new, more effective methods for information security can be developed.