Lecture №1.9.
Main threats for a data security. Methods and tools for the data security..

By its conversion the ***cryptology*** (kryptos - secret, logos - a science) is engaged in a problem of the information protection.

The cryptology is divided into two directions - *cryptography* and *cryptanalysis*.

The purposes of these directions are directly opposite.

The message consists of the opened text. Process of conversion of the opened text on purpose to make not clear its sense for strangers is named as ***encoding***. As a result of message encoding the cod-text turns out.

Process of reconversion of the cod-text in the opened text is named ***decryption***.

Science, which learns, as it is necessary to arrive to save the maintenance of messages in secret, is named as ***cryptography***.

The people who are engaged in cryptography, call ***cryptographer***.

Cryptanalysts are experts in the field of cryptanalysis - sciences about opening of cods, which answers a question on how to read the clear text disappearing under the coded.

The section of a science uniting cryptography and cryptanalysis, is named by ***cryptology***.

The cryptography is engaged in search and research of mathematical methods of information conversion.

Sphere of interests of cryptoanalysis - research of the information possibility decoding without knowledge of keys.

The modern cryptography includes four large sections:

1) Symmetric cryptosystems.
2) Cryptosystems with opened key.
3) Digital signature systems.
4) Control of keys.

The main directions of usage of cryptography methods - transmission of the confidential information on data links (for example, e-mail), authenticity installation of the transferred messages, the storage of information (documents, databases) on carriers in coded type.

The cryptography gives the chance to transform the information in such a manner that its restoring probably only at knowledge of a key. As the information which are subject to encoding and decoding, the texts constructed on some alphabet will be considered. These terms are understood as the following.

The alphabet - a finite set used for information coding signs.

The text - the arranged set from alphabet units.

As examples of the alphabets used in modern intelligence systems it is possible to result the following:

* alphabet Z33 - the 32 characters of the Russian alphabet and a blank;

* alphabet Z256 - the characters entering into the standard codes ASCII and KOI-8;

* the binary alphabet - Z2 = {0,1};

* the octal alphabet or hexadecimal alphabet.

Encoding - transforming process: the source text which carries also the opened text name, replaces a text in code.

Decoding - return to encoding process. On the basis of a key the text in code will be transformed in initial text.

Key - the information necessary for unobstructed encoding and decoding of texts.

The cryptography system represents T set of conversions the opened text. Members of this set are indexed, or are designated by k character; parameter k is a key. Space of keys K is set of possible values of a key. Usually a key represents a consecutive number of the alphabet characters.

Cryptosystems are divided on ***symmetric*** and ***with opened key***.

In symmetric cryptosystems both for encoding and for decoding the same key is used.

In systems with opened key two keys - the opened and the closed are used, which mathematically are linked with each other are used. Information is encoding by opened key, which it is accessible to all interested persons, and is decoding by closed key known only receiver of message.

Terms keys allocation and keys control concern to processes of information processing systems, by the contents of which compilation and distributing of keys between the users.

The electronic (digital) signature is called the cryptographic transformation attached to the text which allows at text reception by other user to check up authorship and authenticity of the message.

Cryptofirmness is named code characteristic, which defining its firmness to decoding without knowledge of a key (i.e. cryptoanalysis). There are some indicators of cryptofirmness, among which:

* quantity of all possible keys;
* mean time, necessary for cryptoanalysis.

Transformation Tk is defined by corresponding algorithm and an option value k. Efficiency of encoding for the purpose of information protection depends on preservation of secret of a key and cryptofirmness the code number.

Cryptography protection provides data protection of any type, stored in any kind on any carrier, irrespective of the operating system, data format and so forth It there can be disk files, messages of e-mail, record of a database and the other information. Resources of cryptography protection can be built in applications (for example in mailers) or to function as the independent application coding files on the computer of the user. Cryptography resources also can be used for creation of confidential virtual circuits of data transfer, providing either hardware, or the program data encoding, transferred between two network nodes Internet.

Systems of cryptoprotection are realized by two primary tasks.

1) Provide privacy of data, allowing to get access to contents of files, messages and so forth only to the persons owning private keys.

2) Guarantee authenticity of authorship of the information and confirmation of that the information has not been updated by someone another after its publication.

Modern systems of cryptoprotection lean against three base algorithms.

Information encoding can is carried out by means of two algorithms: encoding by means of symmetric keys and encoding by the asymmetric keys, also named algorithm with usage of an open key.

Support of a guarantee of authenticity of the information and the authorship certificate is carried out by algorithm of a digital signature.

Process of cryptographic closing of data can be carried out as program, and is hardware. Hardware realisation differs essentially bigger in cost, however advantages are inherent in it also: high efficiency, simplicity, security etc. Program realisation is more practical, supposes known flexibility in use.

For modern cryptographic systems of protection of the information the following standard requirements are formulated:

- The coded message should give in to reading only in the presence of a key;

- The number of the operations necessary for definition of the used key of encoding by a fragment of the encoded message and an opened text corresponding to it, should be not less the general number of possible keys;

- The number of the operations necessary for decoding for the information by search of every possible keys should have a strict bottom estimation and to leave for limits of possibilities of modern computers (taking into account possibility of use of network calculations);

- The knowledge of encoding algorithm should not influence reliability of protection;

- Key minor alteration should result in essential change of sort encoding messages even at the usage of the same key;

- Structural elements of algorithm of encoding should be invariable;

- The additional bits entered into the message in the course of encoding, should be completely and are reliably hidden in a text in code;

- The length of a text in code should be to equal length of the initial text;

- There should not be simple and easily established dependences between the keys, consistently used in the course of enciphering;

- Any key from set of the possible should provide reliable protection of the information;

- The algorithm should suppose both program, and hardware realisation, thus change of length of a key should not conduct to qualitative deterioration of algorithm of enciphering.

The cryptography algorithm also named as the cod or algorithm of encoding, represents the mathematical function used for encoding and decoding. If to be more exact, such functions two: one is applied to encoding, and another - for decoding.

Thank you for your attention