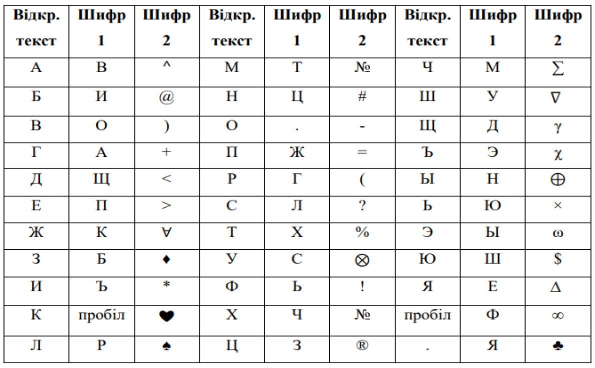
***T. Verhun, Lecturer***
***M. Kukulivskiy, Student***
*Zhytomyr Polytechnic State University*

# CRYPTOGRAPHIC PROTECTION OF INFORMATION

The aim of this study was to investigate the problem of protection of information networks. In particular, attention is drawn to the lack of timely intervention in cases where the reliability of data transmission and its content is at risk. Human intervention can be both untimely and ineffective. Also, one should not forget about the human factor, negligence, incompetence of personnel, which can nullify the technical potential of even the most advanced information protection systems. In order to protect an uninitiated person from incorrect actions with information technologies, the doctrine of information protection, called cryptography, can be used.

Cryptography is the science of mathematical methods of ensuring confidentiality, integrity and authenticity of information [1].

As an example, I suggest you familiarize yourself with the replacement table for two ciphers (Fig. 1).



| Відкр. | Шифр | Шифр | Відкр. | Шифр | Шифр | Відкр. | Шифр | Шифр |
|---|---|---|---|---|---|---|---|---|
| текст | 1 | 2 | текст | 1 | 2 | текст | 1 | 2 |
| А | В | ^ | М | Т | № | Ч | М | ∑ |
| Б | И | @ | Н | Ц | # | Ш | У | ∇ |
| В | О | ) | О | . | - | Щ | Д | γ |
| Г | А | + | П | Ж | = | Ъ | Э | χ |
| Д | Щ | < | Р | Г | ( | Ы | Н | ⊕ |
| Е | П | > | С | Л | ? | Ь | Ю | × |
| Ж | К | ∀ | Т | Х | % | Э | Ы | ω |
| З | Б | ♦ | У | С | ⊗ | Ю | Ш | $ |
| И | Ъ | * | Ф | Ь | ! | Я | Е | ∆ |
| К | пробіл | ♥ | Х | Ч | № | пробіл | Ф | ∞ |
| Л | Р | ♠ | Ц | З | ® | . | Я | ♣ |

Fig. 1. Substitution table for two ciphers

Depending on the presence or absence of a key, coded algorithms are divided into cipher and cryptography. Depending on the correspondence of the encryption and decryption keys - symmetric and asymmetric. Depending on the type of transformations used - wildcards and permutational. Depending on the size of the encrypted block - into stream and block ciphers.

Regarding crypto-algorithms, there are several classification schemes, each of which is based on a group of characteristic features. Thus, the same algorithm "passes" through several schemes at once, ending up in any of the subgroups in each of them.

The main scheme of classification of all crypto-algorithms is as follows:

- Cryptography. The sender and receiver perform a transformation on the message that is known only to the two of them. The encryption algorithm itself is unknown to outsiders.

- Key cryptography. The algorithm of influence on the transmitted data, which is known to all third parties, but it depends on some parameter - the "key", which only the sender and the recipient have.

- Symmetric crypto-algorithms. The same block of information (key) is used for encoding and decoding a message.

- Asymmetric crypto-algorithms. The algorithm is such that one ("open") key is used to encrypt the message, known to everyone, and another ("closed") key is used for decryption, which exists only for the recipient.

The work shows that throughout its history, humanity has needed encryption of one or another information. A whole science - cryptography - grew out of this need. Previously, cryptography served only the interests of the state, but with the advent of the Internet, private individuals became interested in its methods [2].

Today, cryptography is widely used not only by hackers, but also by fighters for freedom of information, the financial sector, military structures and ordinary users who want to protect their data on the network. The relevance of cryptography will not fade in the coming centuries.

## Protection of the SAP system

The structural diagram of the complex according to the placement of its constituent parts on separate technical means is shown in the figure.

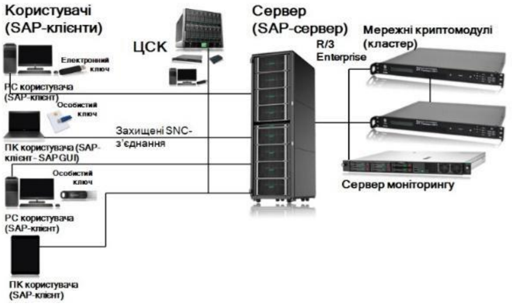


Fig. 2. Protection of the SAP system

The complex includes:

- the SAP client protection software complex "IIT SAP Protection. Client" consists of:
- SNC libraries (connection protection libraries) for the SAP client;
- SSF libraries (secure storage and forwarding libraries) for the SAP client;
- CSK user libraries in accordance with the CSK user software complex "IIT User CSK-1";

the SAP server protection software complex "IIT SAP Protection. Server" includes:

- SNC libraries for the SAP server;
- SSF libraries for the SAP server;
- CSK user libraries;
- server protection management tools;
- SAP server protection monitoring agent;
- software package for remote monitoring of SAP server protection "IIT SAP Protection. Remote server monitor".

KZI software implements the complex operation logic and is integrated directly into the client and server parts of the SAP system (SAP client and SAP server), through the mechanisms and interfaces of cryptographic information protection defined in the SAP system. Software tools of the KZI complex can use external hardware tools of the KZI, such as electronic keys, network cryptomodules, etc [3].

SNC libraries (connection protection libraries) as part of the SAP client and SAP server are designed to implement authentication mechanisms for users of the SAP system on the server during user connection to the server (establishing a connection with the server), by implementing the mutual authentication protocol parties, and ensuring the confidentiality and integrity of information transmitted between users and the SAP system server during their interaction, by encrypting information and forming and verifying cryptographic checksums.

## REFERENCES

1. Ceit Blog (2023). Retrieved from: http://ceit-blog.ucu.edu.ua [in Ukrainian]
2. KPI (2023). Retrieved from: https://ames.kpi.ua [in Ukrainian]
3. KUBG (2022). Retrieved from: https://csecurity.kubg.edu.ua [in Ukrainian]