DISCLAIMER INFORMATION SAFETY IN THE UNIVERSAL EDUCATION AND INFORMATION IN THE EDUCATION

Erkayev Husan Ahmadaliyevich & Primkulova Alima Asetovna
Teachers of the Department of Information Technology of TSPU
Tashkent city

ABSTRACT

This article discusses the concept of information security in the system of continuing education, discloses methods of information protection in pedagogical activity.

Keywords: Education, information technology, modern technology, computer games, communication, independent movement, speech culture, the Internet, electronic information.

INTRODUCTION, LITERATURE REVIEW AND DISCUSSION

In today's world, all attention is focused on information security, and many people realize the importance of information security. The doctor, the teacher, the entrepreneur, the accountant or the lawyer - all have their own secrets that they do not want to disclose. These are the secrets of the service.
In order to be informed, it must have three qualities:
- The information must be complete;
- Data must be reliable;
- Information must be valuable in a certain sense;
Once the data is of this quality, they will become information. The information is divided into two types of information, both public and private, in storage and use.
We may obtain open data from print and internet sources, including unrestricted access to users. Confidential information is different from the fact that it has a range of users and that there is a risk of exposure. This classified information is classified as: state secrets, military secrets, scientific research secrets, and service secrets [1].
As the information security, this confidential information is protected.

We can list the following as protection methods; Physical protection, legal protection, mechanical and hardware protection, hardware and software protection, and cryptographic protection. Today, it is possible to effectively use these methods of information protection, for example, to store information safely and to limit the number of people who can access this information, to use protected buildings. is possible. Such data protection tools have their disadvantages as well as their disadvantages, which can be seen in the process of information exchange. Here are some of the ways we can protect your information:
- protection of data communication networks;
- masking or transferring confidential information in the open communication network with any other information in the open communication network, ie using stegonographic methods;
- exchange of pre-agreed public information with a hidden meaning between its subscribers;
Unlike the aforementioned methods, cryptography does not hide the confidentiality of the transmitted data, but merely substitutes it for what cryptocurrency does not understand. This is where the communication network is fully controlled by the cryptocurrency. The problem of switching the view of the open data being transmitted is one of the issues that need to be solved among the users of the communication network, and the other side is the authenticity of the

data transmitted and received during the data exchange and the authenticity of the users. make sure To solve this problem:
- authentication, authentication of users and data;
- it is important to ensure that interactions are recorded and prevented by any intentional act by the parties exchanging information to harm or mislead one another;
In order to solve these problems, cryptographic methods can provide the ability to detect any behavior that has been previously performed, and to detect it when misleading. Therefore, modern cryptography is the process of exchanging information in the communication network:
 confidentiality (confidentiality);
Liq completeness (unchanged determination);
 authentication (user authentication);
 oldini Ensure that parties do not recognize co-authorship;
Yaratish ensuring the generation, distribution and management of keys;
It is a field of knowledge dealing with such issues. The solutions to these issues are the key to cryptography, ensuring the protection of data exchange processes in the network.
We shall dwell on each of the above issues separately.
Confidentiality is to prevent the parties or individuals from accessing this information without the right to read the original content.
Integrity assurance is a guarantee of avoidance of unauthorized changes in the transmission of data.
Authentication is the development of ways to guarantee the authenticity of the parties in the communication network.
Protecting Parties from Authority Denials - Measures to prevent such subjects from failing to acknowledge their actions after a certain period of time [2].
Description. The family of reflective transitions, each of which is defined by a parameter called key, is called a cipher.
Description. Encryption mode for the use of reflection swaps is the opposite.
Description. The key to decrypting the data is the key to decrypting an existing overriding switch.
Usually a key consists of a finite series of characters, letters, or numbers.

Each inverted reflection switch is identified by a single key and is represented by a cryptographic algorithm. The same cryptographic algorithm can be used in different encryption modes. Each encryption mode, in turn, has its advantages and disadvantages. Therefore, the choice of which mode depends on a particular case, that is, the cryptographic algorithm used in encryption may differ from encrypted data to the cryptographic algorithm used in decryption.
In addition to securing the confidentiality of the information we have just mentioned, another important issue is securing the transferred data, that is, any unauthorized changes to the data stored or transmitted. is to prevent. This problem can be solved by deliberately adding false information to the data transmitted by the device, or by accidental changes due to a network failure. In order to achieve completeness, the data transmitted is used by a special cryptographic algorithm, which is calculated by using a specific cryptographic algorithm, called the totality control. It is the size of the transmitted data. The difference between this method and the "coding theory" method is that the cryptographic algorithm used depends on the secret key, and the problem of unintentionally changing the totality of the control is complex or goes beyond the capabilities of modern computing devices. that is, it is highly unlikely that a cryptocurrency could add false information to the information provided without knowing the secret key or to accidentally change every sign in the information.

Description. The size of the ciphertext, which determines the ability of each cipher to resist an active attack by a cryptocurrency, is called the level of encryption.

Thus, to verify the transmitted M-data completeness, an additional S-data is added to the consecutive M-data (conjuncture), which is called the data authentication code (full control set). S = (M, S) is transmitted through the communication network. This information S = (M, S) is taken from the other side and calculates the totality of the M-data. If the computed bandwidth is equal to C, then M-data is actually accepted without any modifications, otherwise M-data is rejected.
Typically, the S-data authentication code is used as a cryptographic hash function associated with a secret key, that is, h k (M) = S.
Description. The function that reflects the given M-data to a given length is called a hash function.
In turn, there are a number of requirements for hash functions. These requirements include:
1. Without knowing the secret key for the given M data, h k (M) = S cannot be calculated.
2. Given the given M-data and so on (M) = S-hash, it should not be possible to find the same M'-data, resulting in hk (M ') = S, ie it is not possible to find two explicit texts with a hash value [3].

The first requirement is to oppose the creation of one key with counterfeit keys, and the second requirement is to counter the modification of transmitted data.
Generally, the concept of authentication applies to all aspects of the data-driven processes. Examples: communication session, parties, data being transmitted, and more.
Authentication for all parts of the data process is an important part of providing reliable data transmitted. This is especially true in the exchange of information between conflicting parties. Because it is not only the cryptocurrency that is the basis for the threat of information sharing, but also the wrong actions of both parties.
Authentication for a communication session means full connection, timely transfer of data, and prevention of repeated data transfer by a cryptographic analyst.
Additional parameters are used to provide authentication for the communication session. For example: the data to be transmitted is a cryptographic algorithm, including timestamps, random numbers, and serial numbers.
Interoperability Authentication - Verify that any party you want to interact with is actually sharing information with the other party.
In most cases, the parties are also referred to as the parties 'authentication and respectively the parties' identification. This is a formal explanation, which means identification of the parties, usually the procedure for the identification of the parties to distinguish them from other users. In this case, the process of identifying these names is to display or give these names. Therefore, authentication can be called validation of authentication.
Description. The sequence of tasks assumed by two or more parties to solve a practical problem is called a protocol.
The authentication tool is an authentication protocol that provides for the identification (authentication) of trustees.
Identity protocols are of two types:
• One-way authentication protocols.
• Mutual identification protocols.
As a result of the authentication protocol, both parties do not disclose their private key and answer each question (request).

Authentication of the data itself is true of the fact that the information transmitted over the communication network is true, that is, the accuracy of the data transmitted, the time of its preparation and the parameters of the judgment.

If both parties trust each other, this can be done using an encryption algorithm with a public key. However, if the parties express a lack of confidence in each other, then it is necessary to develop a mechanism for resolving the issue. This mechanism is called Digital Signature (EDS), and we will give some comments below.

From experience, it is clear that some people may deny that they have not done anything for their own purpose or behavior (for example, a document) for a long time. The only way to clarify such controversial issues is through digital signature.

Any standard digital signature algorithm available today consists of two parts:

1. Signature Counting section.
2. Signature verification section.

According to the EDS algorithm, only the data owner can sign the data with a private key. All users can check EDS authenticity. Digital signature scheme: can be implemented using both symmetric and asymmetric encryption algorithms.

In the digital signature scheme based on the symmetric encryption algorithm, the signature data is a secret encrypted form. However, the disadvantage of this signature is that the private key is kept secret. This can cause a number of inconveniences, such as always having to choose a new key when signing and only using it once.

There are two types of digital signature generation using asymmetric encryption algorithms:

1. The information provided is fully encrypted with the owner's private key. The signator can verify the signature with the public key.
2. Signature counting is a digital transformation of signature data, and the signature counting algorithm depends on the private key. This is why it is important that the signer be signed only by the owner and anyone can verify it. This is why the signature verification part is compiled by the owner's public key.

It should be noted that if the length of the signature in the first round is determined by the length of the given data, then in the second round, the length of the signature is determined regardless of the length of the data.

When calculating digital signatures in relation to a given data, it is most convenient when the data is first calculated as a hash value and then the sequence of actions specified in the algorithm (EDS). The hash value is calculated using the hash function algorithms, respectively.

LIST OF REFERENCE

1. Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. Изд. 4-е. М.: Ленанд, 2015 г.

2. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на Си. М.: Издательство ТРИУМФ, 2012 г.

3. Варфоломеев А.А. Основы Информационной безопасности. Москва, 2008 г. 412 с.

4. S.K. Ganiyev, M.M. Karimov, K.A. Tashev “Axborot xavfsizligi”. T: «Fan texnologiya», 2017 y. 372 bet.

5. Khasanov A.A. Didactic Foundations of Interdisciplinary Connections at Subject Teaching // Eastern European Scientific Journal. Germany -2018. No. 6. P. 127-130.

6. Xasanov A.A., Mirjamolova F.N. Access to electronic educational resources in the education system // European Journal of Research and Reflection in Educational Sciences Vol. 7. No. 12, 2019. P.442-445.