11th International Conference. September, 10 - November, 30, 2020.
UK, S Yorkshire, Sheffield

«SCIENCE AND PRACTICE: A NEW LEVEL OF INTEGRATION IN THE MODERN WORLD» • Conference Proceedings

DOI: http://doi.org/10.15350/UK_6/11

Research Article

PROBLEMS OF INFORMATION SECURITY

N.S. Sayidova[1]

Z.B. Xo'jamqulova[2]

[1]Docent of the Department of Information Technologies, Bukhara State University, Uzbekistan.

[2]Student, Physics and Mathematics Faculty, Bukhara state University, Uzbekistan.

DOI: http://doi.org/10.15350/UK_6/11.48

Abstract

Article is devoted problems to provide information security and all measures on their prevention, how to protect the information, the basic organisation of information security, and protective functions to define that they stand from identification of function for protection of the software of information security on a technical question, reflecting more detailed information on cryptographic methods of protection. Besides, the information in the elektronno-digital signature for safety of computer viruses is the reliable tool for effective work of the anti-virus software for protection of information systems and components at the same time struggle against attacks on the theoretical data.

Key words: Information security, enciphering, decoding, a digital signature, identification, cryptography, computer viruses, anti-virus program components, the program provided blocks to protect in a complex from external threats.

By information security, we mean information that prevents accidental or unintended adverse effects of a natural or artificial nature that may cause undue harm to information subjects, including those that support their infrastructure, and we understand that information is protected from owners. Information security is a set of measures to ensure the security of information [1]. The main components of information security are the following categories: infrastructure support and ensuring confidentiality, integrity and availability of information resources.

Utility is the ability to obtain the information you need over a period of time. Integrity is the relevance of information and its protection from destruction and unauthorized changes. Only authorized people should be able to change the information. Confidentiality is the protection of information from unauthorized access, to which only authorized persons should have access.

The main method of protecting information is access control, which is a protection method that regulates the use of all resources of information systems and information technologies. Such methods should be able to exclude any unauthorized access to information. Access control includes the following security functions: identification of users, employees and system resources (assigning a personal identifier to each object); identification of an object or subjects by the identifier assigned to them (ensuring authenticity); verification of the right to use; registration of access to protected resources; detection of unauthorized access attempts (alarm warning, system shutdown, system shutdown, refusal to answer requests).

Identification and authentication can be considered as important software and hardware security, since the rest of the services are intended only for subjects. Identity and authentication is the main line of defense against accessing an enterprise's information space. The joint execution of the identification and authentication procedure is considered an authorization procedure. Identification allows subjects (users, processes acting on behalf of a specific user) to identify themselves. Authentication allows the other party to know who they really are. The term "authentication" is sometimes used synonymously with "authentication".

DOI: http://doi.org/10.15350/UK_6/11

There are also cryptographic (Greek secret letters) information security methods, which are a set of ideas and techniques related to modifying information in order to protect information from unintended users. ... The information is presented in the form of text (message). This information is called plain text. The encryption process is called encryption and the encryption process is called encryption.

Conversion from cryptogram to plain text is done by decryption. Additional information called a key is used for encryption and decryption. The exact key is the encryption secret [5]. Reading a cryptogram for a limited period of time without knowing the key should be significantly more difficult or practically impossible. Cryptography is one of the components of cryptology, the science of transferring information protected from unauthorized access.

Cryptography, as it is also called, encrypts and decrypts data using a secret key. Another component of cryptology is cryptanalysis, which deals with the theory of extracting information from a cryptogram without knowing the key [4]. Modern cryptography consists of four main sections: symmetric cryptosystems; public key cryptosystems; electronic digital signature systems, key management.

Electronic digital signature (EDS) is a property of an electronic document that is used to protect an electronic document from counterfeiting and verify the source of information. An electronic digital signature consists of a sequence of characters created by cryptographically modifying an electronic document. ERI joins the data block, allowing the recipient of the data to protect the data source, data integrity from fraud. An electronic digital signature is created by cryptographic modification of information using special software and a secret key of an electronic digital signature.

EDS improves electronic document exchange and ensures document reliability. If the original text is changed arbitrarily, the EDS will not be valid. A single public and private cryptographic keys are generated for each user participating in the exchange of electronic documents and using an electronic digital signature. An important element is the secret key: it encrypts electronic documents and creates an electronic digital signature [2].

In addition, the secret key remains with the user and is delivered through a separate medium: it can be a floppy disk, a smart card. You will need to keep it private to other users on the network. The public key is used to check the validity of the EDS. A copy of the public keys is kept at the authentication center. The Authentication Center ensures registration and protection of the public key against errors or attempts to forge. Information security also includes anti-virus protection [3].

Thus, to effectively combat malware requires a comprehensive approach to protecting against external threats to information security. There are four main types of software for protection against external threats to information security in the information technology market: antivirus software; corporate firewall; personal firewalls; attack protection is one of them. Their application on site will definitely ensure your information security.

References

Zaripova G.K. Обучения студентов компьютерным технологиям. Российкая федерация. «Готовим урок». – Курск: – 2016 г. 30 июнь. Свидетельство о регистрации СМИ: ЭЛ № ФС 77 – 65563. http://gotovimurok.com/?page_id=28459

Зарипова Г.К., Сайидова Н.С., Норова Ф.Ф., Абдуакҳадов А.А. Features of the credit and modular system in higher education. «Асадемй». Российский импакт–фактор: 0,19. Научно–методический журнал. № 10 (61), 2020. 25–29–стр.

Сайидова Н.С., Зарипова Г.К., Абдуахадов А.А., Журакулов Ж.Ж. Использование электронных ресурсов в историческом образовании и его защита. «АЭТЕРНА» научно-издательский центр. Научный-электронный журнал «Академическая публикация" №2, 2020 г. 123–131–стр.

Сайидова Н.С., Нематов Л.А. Теория и методика профессионального образования. Образование и проблемы развития общества научно-практический рецензируемый журнал. Г. Курск. Россия. №1(7) 2019 год. 55-59-Р. (ISSN 2411-9792)

Сайидова Н.С., Казимова Г.Х. Разработка методики образования в вузах. Образование и проблемы развития общества научно-практический рецензируемый журнал. Г. Курск. Россия. №1(7) 2019 год. 36-40-Р. (ISSN 2411-9792)

DOI: http://doi.org/10.15350/UK_6/11

Ismoilova M.N., Imomova Sh.M. Function interpolation // BULLETIN OF SCIENCE AND EDUCATION 2020. No. 3 (81). Part 3. C.5-8.

Imomova Sh.M., Ismoilova M.N. Calculation of the largest eigenvalue of a matrix and its corresponding eigenvector in the Mathcad environment // ACADEMY. No. 6 (57), 2020. C.9.

Imomova Sh.M., Ismoilova M.N. Numerical solution of a mixed problem, formulated on a vector wave equation in a domain with an angle // UNIVERSUM: TECHNICAL SCIENCES. No. 10 (79), 2020. S. 22-25.