



THE IMPORTANCE OF INFORMATION LEARNING ENVIRONMENT IN THE FORMATION OF VOCATIONAL SKILLS AMONG STUDENTS OF VOCATIONAL EDUCATION SYSTEM

Botirova Nigora Koyirovna

Institute of Retraining and Professional Development of the
Staff of Bukhara Regional Public Education

Abstract

Education is one of the main pillars of the development of the state and society. The rapid development of society on a global scale-forms an age of globalization and informatization. The article provides information on the role, relevance and importance of the science of "Information security" in the formation of professional skills of students of the system of vocational education.

Keywords: electronics, vocational education, information, knowledge, qualification, information security, confidentiality, cryptography, authorization, integrity, identification, authentication, electronic digital signature, password.

Introduction

In the process of theoretical vocational education, which is carried out in secondary specialized professional educational institutions, a system of theoretical knowledge and skills is formed, practical skills are formed in the process of practical vocational education. As a product of both these processes, a specialist personality with a certain profession and qualifications is formed.

Professional education in the Republic of Uzbekistan – taking into account the prospects and priorities of the development of the economy, modern technical and technological trends, the Real need for personnel in the labor market, proposals of employers and is intended for the education of individuals on the basis of the printing "Obtaining education throughout life".

The purpose of professional education is to prepare competitive personnel for the needs in the labor market, including small business and private entrepreneurship, through the introduction of professional training stages, as well as meet the requirements of individuals of different ages to receive education on the basis of the "Life-long education" print-out.

In the world, the electronization of the educational system, the use of electronic educational resources in the teaching of subjects, the improvement of their methodological supply, the formation and development of students' professional





skills, the conduct of training through multimedia and pedagogical software are being studied.

The rapid development of science, the rapid updating of technology, the increase in the number of media sources, the organization of the educational process on the basis of modern pedagogical and Information Communication Technologies, the effective use of educational didactic means, the conduct and evaluation on the basis of international evaluation programs are considered important areas.

In our country, measures are being taken to ensure the active development of the digital economy, the broad introduction of modern information and communication technologies in all sectors and fields, primarily public administration, education, health and agriculture.

Improvement of personnel training system in the field of information technologies is one of the important conditions for successful implementation of the strategy "Digital Uzbekistan – 2030", development of digital technologies and wide introduction into the daily life of the population.

The development of digital technologies is due to the high need of information access by the people of different professions, who are members of our society, to increase their culture of information access, the use of electronic media sources, lack of trust in various unfounded sources, knowledge, qualifications and skills in information security and their protection.

In our republic, several specialties in the field of network and spheres are being trained in the direction of Informatics and information technologies preparation of secondary-special professional education system. In particular, it includes computer engineering, device and software configurator, computer graphics and design operator, information machine tools and computer networking operator, software engineering, information security, programming in computer systems and computer networking specialties etc. In the curriculum of all the above specialties there is a subject "Information Security".

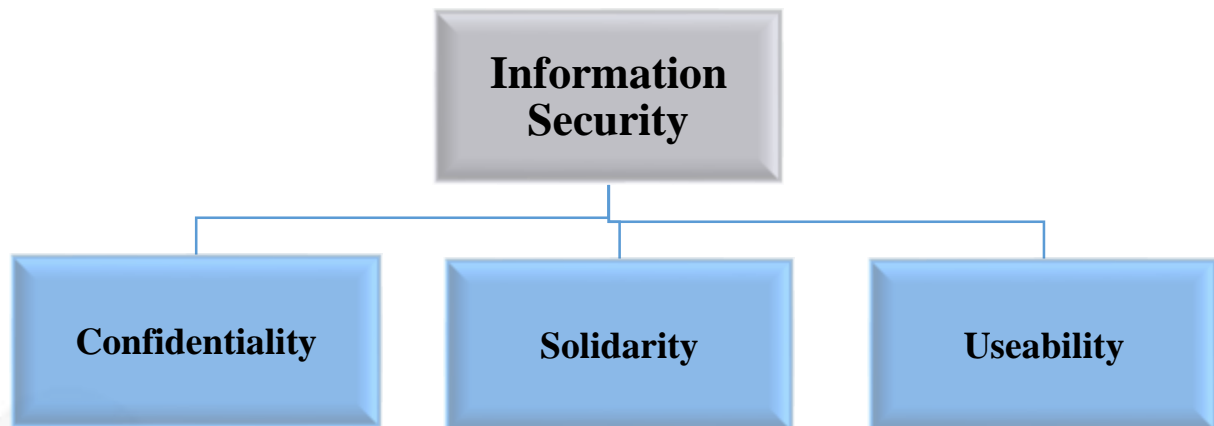
We came to such a conclusion on the basis of the analysis of scientific and methodological literature, the development of Internet and Internet technology systems, the impact of information exchange through mass media and communication technology, the high need for the use of information from different professions in the field of digital technology in various fields, in particular management, social activities, education and economic fields, increasing the culture of their collection, storage, editing and dissemination, the problems of Information Security, which today is the demand of the era, should be viewed as a serious problem.





Based on this point of view, we tried to describe the content of theoretical and practical education in the subject of "Information Security" in the system of secondary special professional education and to describe its basic set of terms and concepts.

Умумий ҳолда ахборот хавфсизлиги концепсияси учта ташкил этувчидан иборатлигини эътиборга олинса, ахборот хавфсизлигини таъминлаш деганда маълумотнинг қуйидаги учта хусусиятини таъминлаш тушуниш мумкин.



Information Security Features

In the study of the science of information security, there are a number of terms. In it, it is desirable that the percentage of students knowing the content of explanatory terms is as follows:

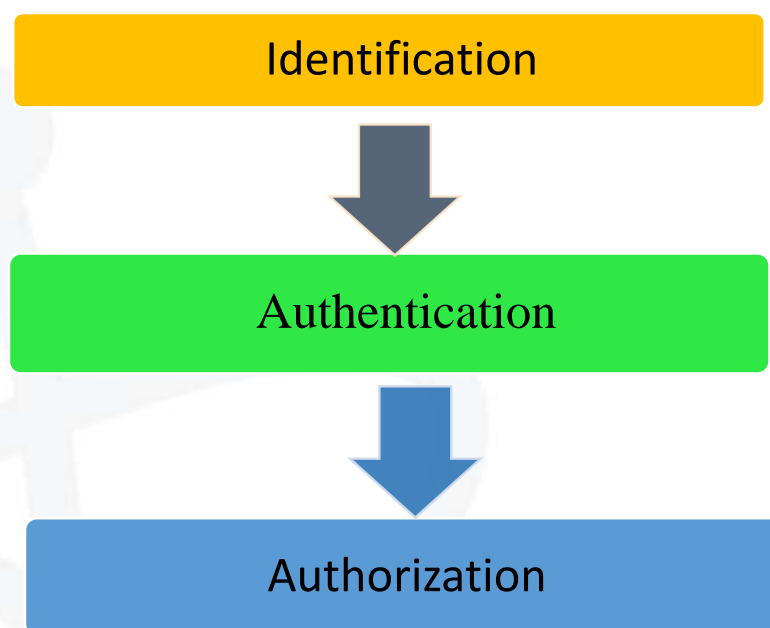
Confidentiality (unauthorized studying is not allowed) – hiding from unauthorized users of information is carried out by performing tasks such as transferring it to an incomprehensible state, so as not to understand the meaning of information. This feature of information is considered one of the methods of cryptographic protection, it is carried out on the basis of encryption methods. With the help of encryption methods, it turns into a state of visible cryptmatn, which is clearly hidden. This will prevent it from corrupting use. It is important for students to have knowledge of this data in the account of about 90 percent.

Integrity (it is impossible to write without permission) On the basis of the integrity feature, it is determined that changes were made or were not made to the data during the transmission. When this feature is said differently, it means that the information has been altered (changed, deleted) by the attacker. This feature of information is carried out with the help of cryptographic methods of protection. Currently, methods for ensuring the integrity of information on the basis of



cryptographic hash functions are widely used in practice. About 70 percent of this information should be known by students.

Useability is determined by the availability of the opportunity to use information at any time. This feature is a preliminary requirement for open type information. One of the attack methods that can cause this feature to be compromised is DOS (Denial of Service) or its formalized appearance is DDOS (Distributed Denial of Service), which means that this attack method will cause the system to fail in its useability character. Our students need to have a 97 percent level of knowledge about this information. These three characteristics are understood to be the main organizers of Information Protection, providing basically the same three characteristics when it comes to Information Protection. But for these three features to be fully implemented, several work that can be done is required. In other words, before fulfilling these three characteristics, you will have to perform the following operations.



Use Management

Identification – this is the process of self-promotion of the user to the system, in which it is possible to use the user's name (login), special personal cards or biometric properties.

Authentication – this is the process of verifying the authenticity of the users, and as a result of the process, the user receives or is not allowed to use the system. Usually divided into 3 types:





- On the basis of knowing something. For example: password, PIN, question-answer, etc.
- On the basis of possession of something. For example: ID card, security tokens, etc.
- The existing shiga is a typical factors. For example: fishermen, ace, DNA, voice, movement, etc.

Authorization – this is a set of rights granted by the system to the user, which determines the functions that the user can perform within the system. As for this information, our students should have knowledge, qualifications and skills with an indicator of 95 percent, albeit partially.

Password – it is the size that is widely used in authentication, which makes it a great convenience to use. However, the endurance is very low.

Cryptographic Key – it is used in authentication and is more durable than password.

Electronic Digital Signature – this electronic document information is generated as a result of a special modification using the closed key of the electronic digital signature, and with the help of the open key of the Electronic Digital Signature, it is possible to determine whether there is an error in the information in the electronic document and to identify the owner of the closed key.

References

1. Ganiev S.K., Karimov M.M., Toshev K.A. Axborot xavfsizligi [Information Security]. 2008.
2. Akbarov D. E. –Axborot xavfsizligini ta`minlashning kriptografik usullari va ularning qullanilishi [Cryptographic methods of ensuring information security and their application] – Toshkent, 2008.
3. Stamp Mark. Information security: principles and practice. USA, 2011.

