# THE COMPLEX OF FACTORS IN IMPROVING THE SOFTWARE AND METHODOLOGICAL PROVISION OF "CYBER SECURITY" SCIENCE TEACHING IN THE PERIOD OF INFORMATION ATTACKS

**Muxtarov F.M.**
TITU NAMED AFTER Muhammad al-Khwarizmi, Associate Professor of Fergana branch,
Independent researcher of TSPU named after Nizami

***Abstract.*** *In this article, the content and tasks of ensuring cyber security during an information attack, the protection of the rights to collect, collect and use information, the relevance and importance of the problem of ensuring information security, causes, information attacks and information security the scientific opinions of our republic and foreign scientists on the field were analyzed, and a subjective attitude was expressed to them.*

***Keywords:*** *information, information security, information attack, information systems, cyber security, fake news, competence, Internet, ensuring the use of information, ensuring information integrity, ensuring information confidentiality.*

Today, it is natural for leaders and employees of every field, pupils, students, all young people to work with social networks, computer technology, search for information and use them. Therefore, the appropriate use of information systems and the development of information systems in the field, in the implementation of useful goals, worldview, artistic thinking, speaking ability, scientific intellectual potential, as well as in other areas of human daily activity, allow to be aware of the world and modern news. will give. In general, working with productive information in everyday life and professional activity increases the scope of growth of this activity. Therefore, when looking for information about the industry, it is important that we take into account that it is positive and highly effective and that it is reliable. In this case, it is necessary to pay attention to the security of information related to the specific purpose we need.

Decision PQ-167 of the President of the Republic of Uzbekistan dated May 31, 2023 "On additional measures to improve the system of ensuring cyber security of important information infrastructure objects of the Republic of Uzbekistan" was adopted [1].

Cybersecurity is a relatively new concept with many different definitions. Specifically, the CSEC2017 Joint Task Force source defines cybersecurity as follows: Cybersecurity is a computationally-based field of knowledge that includes technology, human, information and embodies processes. It includes the creation, implementation, analysis and testing of secure computer systems [3].

The terms "cyber security" and "information security" are often used interchangeably. Some use cyber security as a synonym for information security, information technology security and (information) Risk Management. Others, particularly those in government, view cybersecurity as a technical concept related to national security, which includes cybercrime and the protection of critical infrastructure. Although there are cases of adaptation by various industry personnel for their purposes, there are some important differences between the concepts of information security and cyber security.

The field of information security deals with the protection of intellectual rights regardless of the expression of information - in paper form, electronic and human thinking, verbal and visual communication. Cyber security deals with the protection of information in electronic form (information stored, transmitted and processed in all situations, from networks to devices, in interoperable systems). In addition, attacks funded by governments and advanced persistent threats (Advanced persistent threats, APT) also belong to cyber security. In short, understanding cyber security as a branch of information security helps to understand it properly [4].

S.K.Ganiyev, M.M.Karimov, K.A.Tashayev's confession, "Information security is the prevention of inappropriate (for the relevant subjects of information relations) information disclosure (confidentiality violation), violation (integrity violation), leakage, loss, modification, or usability level. it is characterized by its protection from decline and illegal circulation. The cause of these events may be accidental effects or effects resulting from the deliberate unauthorized use of an infringer (intentional infringer).[5].

Over the following years, the following types of information attacks have become widespread: deliberate criticism of the state's national policy; spread fake news; manipulation of social consciousness; describing a small problem as a big, big problem; distracting students; instilling national values; destroying and changing the historical memory of the people; cyber terrorism.

Based on the modern information system and its wide possibilities, it can be said that it is necessary to create a management mechanism for obtaining, storing, using and distributing information in Uzbekistan from the point of view of national interest and national development, and to deeply understand its essence and elements[2].

Olim Davlatov O.G. In his research on the topic "Development of students' competence to ensure information security through the means of historical and cultural heritage": "Information attack or threat is a set of conditions and factors that threaten the vital interests of the individual, society and the state in the information field" [2], he says.

As long as an information attack is observed, ensuring information security is one of the important issues.

We can explain the relevance and importance of the problem of information security for the following reasons:

- a sharp increase in the computing power of modern computers at the same time as they are easy to use;
- a sharp increase in the capacity of information collected, stored and processed using computers and other automation tools;
- incorporation of various tasks and various related information into a common data base;
- high rate of increase in the price of personal computers used in various fields of activity;
- a sharp increase in the number of users who have access to computing resources and data base;
- development of software tools that do not meet even the minimum requirements of information security;
- mutual distribution of network technologies, integration of local and regional networks into global networks;
- the development of the Internet global network, which almost does not prevent the violation of the security of information processing systems all over the world;
- The ideology of openness and non-control of the Internet global network.

Ensuring information security involves the implementation of multifaceted activities of a regular and complex nature. In its implementation, it is necessary to pay special attention to the tasks set before the parties interested in information security. These various tasks can be divided into the following main groups:

1) ensuring the use of information, i.e. receiving information service within a reasonable period of time and eliminating unauthorized prohibition of receiving information;

2) ensuring the integrity of information, that is, eliminating unauthorized modification or corruption of information;

3) ensuring the confidentiality of information, that is, eliminating unauthorized access to information.

Information protection in modern computer systems and networks means the use of various tools and methods, taking measures and holding events in order to ensure the reliability and integrity of transmitted, stored and processed information.

Data protection is:

• ensuring the physical integrity of information, that is, preventing information elements from being interrupted and lost;

• not to allow the replacement (modification) of its elements while maintaining the integrity of the information;

• prevent unauthorized access to information by unauthorized persons or processes;

• it means that the resources transferred to the owners should be used only in accordance with the conditions agreed by the parties.

Great attention is being paid to filling the Internet information network with national information, which is characteristic of our values, which embody our national identity, and whose reliability is confirmed. For this purpose, a number of projects are being implemented. This, in turn, serves to a certain extent to prevent information attacks and threats. It can be emphasized that it can happen at any time and in any society, but organizing systematic work on its solution in the political, legal, socio-economic and spiritual spheres will increase the cyber security culture.

**REFERENCES**
1. O'zbekiston Respublikasi Prezidentining 31.05.2023 yil PQ-167-sonli qarori.
2. Davlatov O.G'. Talabalarda axborot xavfsizligini ta'minlash kompetentligini tarixiy-madaniy meros vositasida rivojlantirish. Ped.fan.fals…diss. Toshkent-2018. -26 b.
3. Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonized Criteria (1991) Luxembourg: Office for Official Publications of the European Communities, 1991 ISBN 92-826-3004-8, Catalogue Number: CD-71- 91-502-EN-C © ECSC-EEC-EAEC, Brussels Luxembourg
4. Xasanov P.F., Xasanov X.P., Axmedova O.P., Davlatov A.B. "Kripto tahlil va uning maxsus usullari" elektron o'quv qo'llanma. 2010 y.
5. G'aniyev S.K., Karimov M.M., Tashayev K.A. Axborot xavfsizligi. Oliy o'quv yurt talabalari uchun mo'ljallangan o'quv qo'llanma. "Fan va texnologiya" nashriyoti, Toshkent -2016