WEB OF SCIENTIST: INTERNATIONAL SCIENTIFIC RESEARCH JOURNAL
ISSN: 2776-0979, Volume 3, Issue 12, Dec., 2022

HOW TO CREATE CYBER SECURITY WITH DIGITAL TRANSFORMATION IN PUBLIC EDUCATION

O. Pardaev
Senior Lecturer of Karshi branch of Tashkent
University of Information Technology

D. Islamova
Assistant Teacher of Karshi branch of Tashkent
University of Information Technology
Email: O.Pardayev@mail.ru

Abstract

The article discusses the practical importance of information security in the digital transformation of the public education system, the problem of identifying vulnerabilities in information security and ensuring key factors for protecting information from information security incidents.

Keywords: Digital technologies, digital transformation, information security, public education, information security incidents, information security threats, information security protection measures.

An important requirement for ensuring activities during digital transformation in public education is to maintain a high level of information security (Information security). Information security in addition to protecting databases and preventing hacker attacks, it is important to protect students from any manifestations of propaganda and manipulation. Therefore, the construction of an information security system in public education should be carried out by specialists who have the appropriate level of qualification and experience[1]. Information security in the system of a public educational institution is a set of measures of a different nature aimed at realizing two main goals. The first goal is to protect personal data and information space from unauthorized interference, theft of information and changes in the system configuration by third parties. The second goal of IB is to protect students from any kind of propaganda, advertising, information prohibited by law. The actions of intruders can lead to the theft of the specified data. Also, with unauthorized interference, it is possible to make changes and destroy knowledge repositories, program codes, digitized books and manuals used in the educational process. The specifics of providing information security include not only the possibility of theft or damage to data by hackers, but also the activities of students. Teenagers can knowingly or unintentionally damage equipment or infect systems with malware. The following groups of objects may be exposed to threats of intentional or unintentional impact:

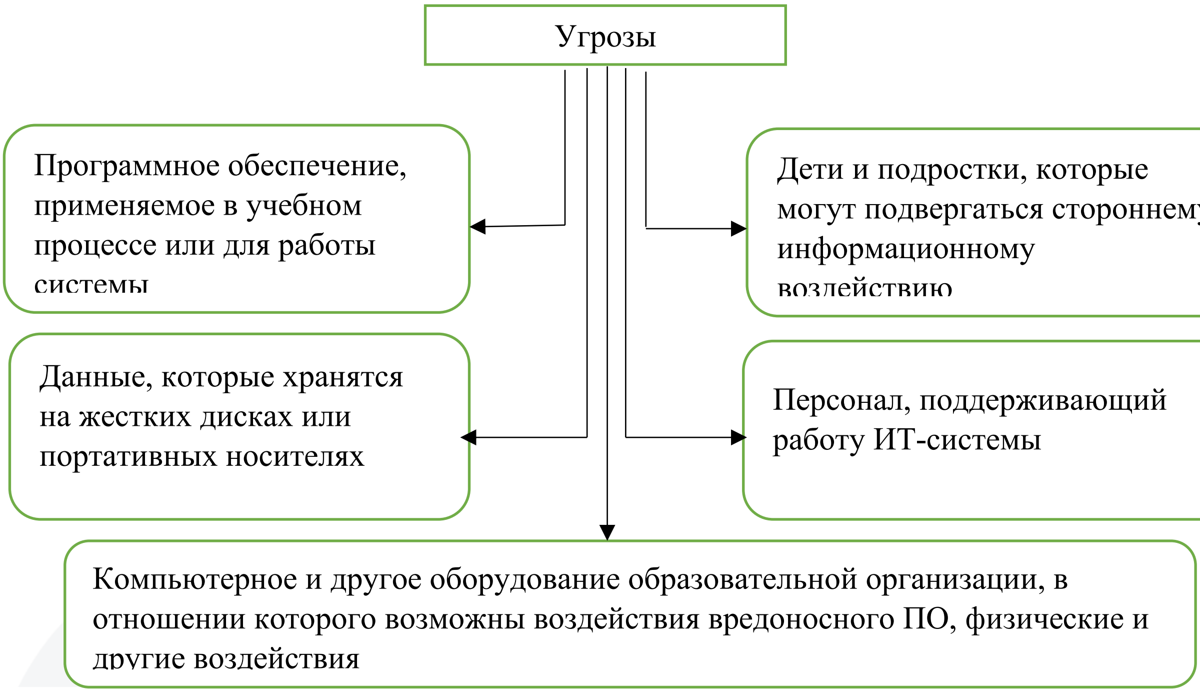
Угрозы
Программное обеспечение, применяемое в учебном процессе или для работы системы
Дети и подростки, которые могут подвергаться стороннему информационному воздействию
Данные, которые хранятся на жестких дисках или портативных носителях
Персонал, поддерживающий работу ИТ-системы
Компьютерное и другое оборудование образовательной организации, в отношении которого возможны воздействия вредоносного ПО, физические и другие воздействия

Fig.1. Vulnerabilities of a group of objects.

In order to provide information security protection measures during digital transformation in public education, information security technologies provide for protection at 5 levels (Fig. 2):

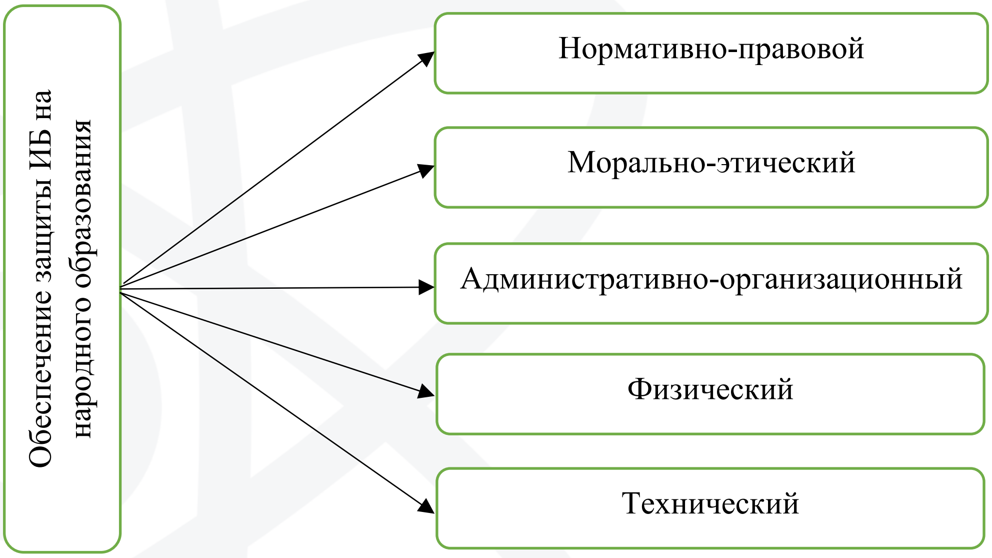
Обеспечение защиты ИБ на народного образования
Нормативно-правовой
Морально-этический
Административно-организационный
Физический
Технический

Fig.2. Measures to protect information security during digital transformation in public education.

1. The legal method of protection is the main document that determines the degree of threats and measures to ensure the information security of students in the public education system, is the "National Strategy for Action in the Interests of Children". It provides for the priority of measures aimed at protecting the child's consciousness from the information impact of an aggressive nature. Measures to protect information systems and databases have a second priority level.

Legislation defines the data that must be protected from unauthorized access by third parties. Such information includes:

- personal data;
- confidential information;
- official, professional, commercial secret.

The procedure for ensuring the security of personal data is regulated by the Labor Code, the Civil Code, the Law "On Information" and other acts.

Moral and ethical means of ensuring information security - this system of moral and ethical values is of particular importance in the field of public education. It serves as the basis for developing a set of measures aimed at protecting children and adolescents from information that is ethically incorrect, traumatic, or illegal. As part of measures to ensure information security, lists of sources (programs, documents, etc.) that can injure a child's psyche are created. As a result of the measures taken, the access of such sources to the territory of the public educational institution system should be prevented.

Administrative and organizational measures - the system of administrative and organizational measures is based on the internal regulations and rules of the organization, which regulate the procedure for handling information and its carriers. The following should be developed, among other things:

- job descriptions;
- internal IS methodologies;
- lists of non-transferable data;
- regulations for interaction with authorized state bodies on requests for information, etc.

The developed methods should determine the procedure for students to access the Internet during classes in computer classes, measures to prevent children from accessing certain resources, preventing them from using their storage media, etc.

Physical measures - the responsibility for the implementation of measures to protect the computer network and physical information carriers lies directly with the head of the educational organization and its IT staff. It is not allowed to shift these measures to hired security structures[4].

Physical measures include:

- implementation of a pass system for access to premises where data carriers are located;
- creation of an access control and management system;
- definition of tolerance levels;
- creating rules for mandatory regular copying of critical data to hard drives of PCs that are not connected to the Internet.

Technical protection measures include the use of specialized software that effectively detects IS threats and ensures the fight against them. If it is impossible to use such systems due to budgetary restrictions, recommended and permitted antiviruses and other types of special software are used. The software used for technical protection must provide control over the e-mail used by students or staff of an educational organization.

REFERENCES

1. Gafner, VV Information security. - M.: Phoenix, 2019.
2. Information security of children. Russian and foreign experience / L.L. Efimova, A S. A, Kocherga. - M.: Unity-Dana, 2017.
3. Information security and information protection / V.P. Melnikov, S.A. Kleimenov, A.M. Petrakov. - Moscow: Higher School, 2019
4. Manako A. F. K. M. Sinitsa CT in education: a look through the prism of transformations // Educational Technologies and Society. – 2012