УДК 004.56
Denys Rybkin[1], Nataliia Zhukova[2]
[1]student of group CST-520, National University «Zaporizhzhia Polytechnic»
[2]PhD (Philology), assistant prof. National University «Zaporizhzhia Polytechnic»

THE IMPORTANCE OF CYBER SECURITY IN EDUCATION SYSTEM

Cyber security is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems from malicious attacks designed to access, alter, delete, destroy or extort them.

Implementing effective cyber security measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative. The speed of technological change results in new risks, requiring new solutions.

The education sector needs to secure its applications and systems and overcome any challenges that come in the way of cyber security. The sector is prone to Distributed Denial of Service (DDoS) attacks which are very common. In the past,

several instances of students or teachers performing a DDoS attack have surfaced with all kinds of motives right from demanding a day off to protesting against something. Other than that, there is data theft that can potentially affect all levels of education. Now at risk: financial data, personal data, enterprise data, educational data. This data can be wrongfully used to sell information or to extort money.

All the most popular social media platforms, such as Facebook, Instagram, Twitter, and LinkedIn are subject to various risks. The authenticity and accuracy of information in this virtual space can be disputed, so that children need to be equipped to protect themselves and take responsibility when facing cyber threats.

The Joint Information Systems Committee report identifies the following challenges:

1. lack of resources and budget (potentially pointing to the lack of finances to invest in cyber security, be it software or staff);

2. cultural issues (a 'Bring Your Own Device' culture is common in Educational institutions and can present difficulties in securing the wider network, particularly with IT staff already facing stretched resources);

3. absence of policy (setting out policies for using the network and making sure they're adhered to can be difficult in large institutions with a dynamic user population).

The challenges schools face in implementing cyber security education include lack of expertise, funding, and resources. Teachers need to enlarge and update their knowledge and expertise regarding cyberspace. Schools and government may lack resources and facilities to implement cyber security education. This is a major obstacle for teachers, as they lack access to learning materials and need to be sensitive to technological change.

In order to prevent cybercrimes in the educational context, it is necessary to provide basic training for all users (young people, teachers, parents). Special education courses must prepare pre-service teachers to design and teach cyber security topics and safe computing methods, the ethics of cyberspace, as well as the ways to keep themselves careful and secure online. Cyber Security awareness workshops are one of the best techniques that can promote cyber security education at schools.

What is more, the academic community and corporations need to team up. Knowing what corporations are looking for in an IT professional and what the company's needs are, the academic community will be able to come up with the curriculum that meets those needs and ensure that college graduates possess the knowledge, skills, and cyber security capabilities to handle the new challenges associated with the digital age.