CONCEPTUAL AND STRATEGIC ASPECTS OF THE FORMATION OF A CYBERSECURITY CULTURE IN THE MODERN ERA

Batirov Farkhod Avazovich,
Head of the Educational process-planning department, Educational and methodological department,
University of Public Safety Republic of Uzbekistan
farxod-batirov@mail.ru

ABSTRACT

Conceptual and strategic aspects of the formation of a cybersecurity culture in the modern era are widely covered from a scientific point of view in the article, which provides the following. In a rapidly globalizing world, ensuring information security and cybersecurity is becoming a key issue both at the national and international levels, creating favorable conditions for young people so that they can easily and correctly understand relevant knowledge and concepts in the field of cybersecurity, while strengthening the legal education of young people and helping them to form the right values in the field of cybersecurity.

Keywords: *cybersecurity, cybersecurity culture, cyberspace, Internet, social networks, information technologies and communications.*

АННОТАЦИЯ

Концептуальные и стратегические аспекты формирования культуры кибербезопасности в современную эпоху широко освещены с научной точки зрения в статье, в которой говорится следующее. В стремительно глобализирующемся мире обеспечение информационной безопасности и кибербезопасности становится ключевым вопросом как на национальном, так и на международном уровне, создавая благоприятные условия для молодых людей, чтобы они могли легко и правильно понимать соответствующие знания и концепции в области кибербезопасности, одновременно укрепляя правовое просвещение молодежи и помощь в формировании у нее правильных ценностей в сфере кибербезопасности.

Ключевые слова: *кибербезопасность, культура кибербезопасности, киберпространство, Интернет/социальные сети, информационные технологии и коммуникации.*

INTRODUCTION

As a starting point for the formation of a culture of cybersecurity in our country, it is important to acquire the knowledge of young people on cybersecurity. Today's

Internet has become a prerequisite for the normal functioning of the world. However, with the application and development of Internet technology, many network security problems began to appear, and their astonishing destructive power led to countless irreparable huge losses. They look like ghosts hiding in the dark, waiting for opportunities, always threatening everything in cyberspace. Under these circumstances, cybersecurity education to adolescents gradually became a major issue of concern to the community as a whole.

Particular attention should be paid to the following according to resolution 57/239 of the UN General Assembly of December 20, 2002 in the formation of a culture of global cyber security:

The rapid development of Information Technology has changed the approach of individual users to cyber security, creating, owning, managing, providing services and using public bodies, enterprises and other organizations and information systems and networks.

Global cybersecurity culture requires all participants to adhere to the following nine complementary elements:

a) to be an officer. Participants should be aware of the need to ensure the safety of Information Systems and networks and what they can do to improve security;

b) responsibility. Each of the participants is responsible for the security of Information Systems and networks according to their role. Participants must regularly review their policies, practices, measures and procedures and assess their compliance with the environment being implemented;

c) reaction. Participants must take timely and collaborative measures to prevent, detect, and respond to security incidents. They are required to share information about threats and vulnerabilities when needed, and to carry out rapid and effective collaborative procedures in preventing, detecting, and responding to such incidents. This may include cross-border information exchange and collaboration;

d) Ethics. Since information systems and networks are embedded in all areas of modern society, it is necessary for participants to take into account the legitimate interests of others and accept that their actions and non-mobility can harm others (or not).;

e) democracy. Security should be ensured in such a way that it is guided by the values adopted in a democratic society, including freedom of exchange of ideas and ideas, free flow of information, confidentiality of information and communication, proper protection of personal information, openness and transparency;

f) risk assessment. All participants must carry out periodic risk assessment. This makes it possible to identify threats and vulnerability factors; has a wide enough base

to cover key internal and external factors such as technology, physical and Human Factors, practical methodology and third-party services affecting security; allows you to determine the optimal level of risk; it helps to choose the necessary control tools that allow you to regulate the risk of possible damage to Information Systems and networks, taking into account the nature and importance of protected information;

g) Design and implementation of security. Participants should consider security issues as an important element in the planning, design, operation and use of Information Systems and networks;

h) Security Management. Participants must take an integrated approach to security management based on dynamic risk assessment covering all levels of their activities and all aspects of their activities;

i) reassessment. Participants must review and revise information systems and network security issues and make necessary changes to security policies, practices, measures and procedures. At this time, it is necessary to take into account the changes in previous threats and Gap factors and the emergence of new ones[1].

From our scientific research, it is known that the concept of cybersecurity culture refers to the attitude, knowledge, assumptions, norms and values of young people to cybersecurity. They are formed by the vital goals, structure, politics, processes of young people and the technologies of spiritual and moral education at different levels. In the process, cyber security culture should reflect organizational and leadership goals.

The state, society and people's strategy serves to ensure the safe use of modern ICT, increase the level of National Information Security, ensure the security of information infrastructure operating in the public and private sector, including important information infrastructure, as well as to establish and implement measures to ensure information security, personal data, as well as to create more favorable conditions for compliance with human rights and freedoms In a rapidly globalizing world, the provision of information security and Cyber Security has become a major issue both nationally and internationally. Among the factors determining the adoption of the strategy is the recent expansion of technologically multifaceted attacks on the information space of Uzbekistan, including its components.

By cybersecurity level of the Global Cybersecurity Index Uzbekistan ranked 70th in its ranking, which included 194 countries. It is reported that the global cybersecurity ranking is for the first time.

It was announced by the International Telecommunication Union in 2015. Countries are evaluated according to a total of five areas of Cybersecurity — Law,

Technology, organizational measures, cooperation and potential development. 20 points are allocated for each direction, and this is a total of 100 points.

Uzbekistan on legal measures within these directions 19.27 points, 13.56 points for cooperation, 15.68 points for capacity development, 10.05 points for organizational measures and 12.56 points for technical measures. The country thus received a total of 71.11 points. Kazakhstan 31st place in cyber security among Central Asian countries, Kyrgyzstan 92nd, Tajikistan 138th, and Turkmenistan 144th [2].

At present, there is a need for the development of "cloud" services in our country, intensive education against "payment program" attacks, an increase in "insider" threats, the widespread use of "multi-factor authentication" methods to combat cyber threats, and the solution of such urgent and extremely serious problems. Important issues in ensuring cybersecurity further demonstrate the importance of strategy in the development and life of our country. The strategy defines the creation of infrastructure on the basis of modern information technologies in the occupied territories, the implementation of the concepts of “Smart City” and “Smart Village” regional stability and as the main conditions for development, it is important to apply appropriate solutions created in this area on the basis of technologies “Big Data”, “Cloud”, “Machine Learning”. In order to increase the effectiveness of the system of monitoring the introduction of information technologies and communications in accordance with the decisions of the president, the Cyber Security Center has established monitoring of the state of information and cyber security provision in all state and economic management, and in the local state authorities on a Republican scale. Monitoring is carried out in state bodies on organizational issues in the development of the ICT sector (programs, official sites, technical events, personnel training and other ICT activities), Information Systems (introduced information systems and resources, database), information security and cyber security issues, the work carried out is evaluated with a rating and relevant recommendations on the elimination of shortcomings. According to the results of the rating assessment, at the end of 2020, the municipality of Namangan region among the authorities in the Republic was ranked 1st with an indicator of 88 percent. The Ministry of Justice also holds the highest position among the 116 public and economic authorities” [3].

Efforts to form a culture of cyber security using international practices and modern approaches have been strengthened in Uzbekistan. Within the framework of the implementation of the new law of the Republic of Uzbekistan “on information on the individual”, Law No. 547 of July 02, 2019, projects began to be carried out in the direction of mechanisms and training for the protection of personal data in society. Of

great importance is the fact that banks, financial organizations and the population are ready for cyberattacks[4].

The objectives of cyber security culture should be strategic, organizational and risk-appropriate. Young people need to understand what the existing culture of cyber security looks like. People today have to learn how the culture, purpose, values that they live in affect cyber security. It is very important for young people to know the truth about where they start by understanding thinking and behavior, which helps them a lot to figure out where there are significant gaps and to develop a road map for their change. To do this, regardless of the type of Service and the number of employees in our country, all companies must regularly organize cyber security awareness training.

Since young people usually have common features such as low internet use skills, mobile game preference, poor ability to distinguish good from wrong, insufficient self-control, and easy imitation, in an environment with such high access rates and high exposure if adolescents do not have the right understanding of Internet and network security, teachers and parents do not have the right Control and guidance for, it will be very easy to develop behavior from cyberspace, such as exposure to illegal offenses or a predisposition to addiction. "Cybersecurity is a set of situations in which all the founders of cyberspace (i.e. technical devices and users)are protected from any threats and unexpected influences" [5].

It is the internet that prevents the healthy physical and mental development of young people. Bad habits have a serious negative impact on the future personal growth of young people and the long-term development of the country. Cases of harmful harm to young people from the internet and severe consequences such as the Blue Whale game, which has encouraged young people to commit suicide and self-slaughter, have been frequent in recent years. In addition to the "preparation or dissemination"of the act in Article 244-1 of the Criminal Code of Uzbekistan, along with such concepts as "preservation, demonstration", the provisions on the act "committed using telecommunications networks, as well as the Internet world Information Network" were included in this article of the code [6].

The most necessary thing for cultural education on cyber security is to start in childhood, because it not only corresponds to the simple laws of education, but also protects the future and hope of the country and the nation. In order to achieve this goal, it is necessary for the owners of reason in society as a whole to act in harmony. Through in-depth visits, inquiries and discussions, it is necessary that we thoroughly develop and implement cyber technologies in cooperation with local education authorities, based on local conditions.

It is also a much more complex process for young people to carry out cultural education activities on cyber security every day. Such activities should be designed to be lively and fun. In addition to the introduction of teaching methods such as thematic lectures, simulation of scenarios, site visits, various new technologies such as virtual reality technology, electronic technologies can be applied in teaching. Effective improvement of a highly immersive learning environment and learning participation. Teaching activities should not be scripted, but should carefully monitor the events of the daily life of adolescents, fully evoke the resonance of adolescents and allow adolescents to fully feel the fun of the educational process.

Efforts are underway both in our country and abroad to increase youth awareness of cybersecurity. Looking back at the international community, more and more countries are adopting increasing awareness of cybersecurity by adolescents as one of their strategic measures and introducing many measures to constantly strengthen awareness and education of cybersecurity in their adolescents. The European Union and many of its member states consider increasing youth awareness of cybersecurity as one of the essential content of cybersecurity strategy, emphasizing the critical role of increasing youth awareness of cybersecurity in increasing community awareness of shared cybersecurity. For example, “the Austrian National ICT Security Strategy “proposes a strategic initiative” to provide education and training in ICT, ICT security and mediatechnologies in the lower classes of schools and to conduct compulsory ICT training programs for all students”. The “Dutch national cybersecurity strategy” (Second Edition) makes it an important goal to “have sufficient knowledge and skills in cybersecurity” and is implementing an action plan to “create a cybersecurity platform for students”. “Cyber security consists of a set of tools that provide cyberspace, enterprise resources, and user protection, namely strategy, security principles, security guarantees, risk management approaches, activities, professional training, and technology” [7].

Great work has also been done to strengthen youth network security education in our country. The laws set out the responsibilities and responsibilities of relevant agencies, such as cyberspace, the press and departments, as well as the state, society, schools and families should pay attention to improving the internet literacy of minors, protecting legal rights and interests in cyberspace. Adult life is also closely linked to the internet, showing the responsibilities and responsibilities of employees of institutions that can control and manage their behavior on the Internet. In full sequence at each stage of National Education, specific and detailed requirements are made for theoretical knowledge and technical abilities related to network security, which should be taken up by adolescents of each school age. “Cyber security is one

of the important conditions in the development of an information society. The difference between the concepts of information security and cyber security is that the purpose of Information Security is to ensure the state of confidentiality, integrity and usability of information in all directions. In turn, cybersecurity it is only in cyberspace (that is, in the Internet Network, Information Systems, etc.).k.) are a set of security-oriented strategies, principles and guarantees of security and measures and tools implemented through human resources" [8].

In real life, there are still those who consider network security to be a state business, which is still far from them. There is still an objective case in some places where there is insufficient attention to network security education, especially network security. The main reason for adolescents is the fact that the construction of a culture of network security in our country has not yet been completed. In this process, it is important to effectively use the capabilities of the cultural sphere. Culture is the foundation of folk belief, and faith is the backbone of the people's heart. When culture becomes a scientific core value, it is a soft force, such as spiritual strength and charm, and when it is transformed into a cultural industry, it is a hard force, such as material productivity. Consequently, culture is not only a blood vessel of the spiritual heritage of the people, but also a concrete symbol of the power of the country and its own manifestation.

Helpless in hard power, defeated in one fight, weak in soft power, defeated without war. As the information age faces rapid development and new technologies, we must not only face increasing global competition in cyberspace, but also be wary of endless threats to network security. To overcome these problems, joint efforts of the whole society are necessary. Only unchanging trust can be a source of our constant self-improvement. Therefore, we must not only create our own network security culture, but also establish a high level of trust in the network security culture. We tear up the Blades of knowledge and technical tools related to the science of network security, reveal their mildest and most reliable sides, and then skillfully harmonize with them the perfect traditional culture, moral concepts and humanitarian ideas of our country, and seek the truth from the truth, are our firm scientific basis. It is necessary to direct people to correctly understand and recognize the meaning of network security and accurately determine its close connection with themselves. As a result, network security has been sublimated from an abstract subject area to a universal ideological culture that is more convenient for the public to understand and disseminate, and then gradually gained widespread recognition and trust from the mainstream ideology of society, finally becoming a concept that people can use. Ideologies and conceptual criteria and standards of thinking that have a positive

impact on everyday life make us confident in our network security culture. Only in this way can we achieve a comprehensive improvement in the security of the national network.

It is necessary to create favorable conditions for young people to easily and correctly understand the relevant knowledge and concepts of cyber security, while strengthening legal education for young people and helping them to form the right cyber security values. In addition to daily educational activities, more online security books should be published that are suitable for young people of all ages, and new self-media methods should be used to disseminate online security content. Teachers adolescents need to fully understand communication tools and information. Everyone's interest and talent will also be different. Today's youth lives are going through the most active period, with a strong interest or high talent in Computer Science and technology and network security technology. In addition to having a simple network security culture for these teenagers, they must be properly guided so that they have more opportunities to explore and delve into relevant topics while successfully completing their studies. This is how the best “hackers” are often born.

CONCLUSION

Through the various educational and propaganda methods mentioned above, we can become a beacon tower of cyber security culture in the hearts of young people to activate. A single spark can ignite desert fire, while the Beacon's message can spread far and wide. Each lighthouse tower has its own characteristics. They can not only illuminate themselves, but also illuminate teachers, relatives and partners around them. Excellent cultural education and heritage are not only the key to self-education, but also the basis for managing the country and establishing peace in the world. When young people are still passionate about knowledge, sow in their hearts the seed of understanding the safety of cyberspace, and then cover it with a good cybersecurity cultural soil, so that if you wait for the time, this seed will definitely grow, Bloom and bear fruit among the mountains the sprouts of rivers. We will certainly be able to see a group of national pillars of cybersecurity looking into the future with their heads raised high under a clear cyber Sky.

REFERENCES

1. Qonun hujjatlari ma’lumotlari milliy bazasi, 03.07.2019 y., 03/19/547/3363-son; 15.01.2021 y., 03/21/666/0032-son; Qonunchilik ma’lumotlari milliy bazasi, 21.04.2021 y., 03/21/683/0375-son;
2. Mirziyoyev SH.M. Inson manfaatlari va huquqlarini ta’minlash – demokratik jamiyat asosidir // Uning o‘zi. Xalqimizning roziligi bizning faoliyatimizga berilgan eng oliy bahodir. 2-jild – Toshkent: «O‘zbekiston». NMIU. 2018. – B.252.

3. Латипов, Окил. "К вопросу об обучении языкам посредством выявления аналогий." Актуальное в филологии 4.4 (2021).
4. Шереметьева, А. Г., and Р. Р. Атаева. "Вариантность как лингвистический феномен." доктор физико-математических наук, профессор, заведующий кафедрой технологии материалов электроники Московского института стали и сплавов (2018): 217.
5. Rashidova, M. K. (2023). TECHNIQUES FOR IMPROVING CADETS'CONVERSATIONAL SKILLS. *Oriental renaissance: Innovative, educational, natural and social sciences*, *3*(3), 637-640.
6. https://digitallibrary.un.org/record/482184
7. https://bugun.uz/2021/10/12/ozbekistonning-global-kiberxavfsizlik-reytingidagi-orni-elon-qilindi/;