WEB OF SCIENTIST: INTERNATIONAL SCIENTIFIC RESEARCH JOURNAL
ISSN: 2776-0979, Volume 4, Issue 10, Oct., 2023

MECHANISMS FOR CREATING A GREEN AND HEALTHY INTERNET ENVIRONMENT FOR YOUNG PEOPLE IN THE MODERN ERA

Batirov Farxod Avazovich,
Head of the Educational Process-Planning Department,
Educational and Methodological Department,
University of Public Safety Republic of Uzbekistan
farxod-batirov@mail.ru

Annotation

This article is widely covered from a scientific point of view, which states the following. In order to realize the dream of becoming a powerful country with the Internet, we must start educating young people from the “childhood” age. That the government and enterprises should create conditions for the use of the Internet by young people, direct them to active innovation, use their talent. The future of smart cities, the development of e-commerce and Internet technologies, joining the ranks of the world's cybersecurity forces as soon as possible.

Keywords: Information security/ cybercrime/ website/ cyberspace/ Internet / national security / network security.

Intruduction

According to a survey of teenagers in our country on the internet, it has been almost 20 years since teenagers entered the internet. The state has regularly increased its efforts to combat illegal crimes on the internet. Local website providers have significantly increased their knowledge of law-abiding and internal affairs procedures. The internet environment has improved significantly. Parents' concerns about online time and website browsing content have changed from the beginning. Restrictions and restlessness gradually became more rational. Online education and vision requirements in schools also increased youth's ability to differentiate from their own time. General self-management of the wrong online system on the internet and the limitation has improved significantly.

Protection of youth from information threats in Uzbekistan, education on the basis of the development of World Science, President of the Republic of Uzbekistan Shavkat Mirziyoyev said to the world community at the 72nd session of the United Nations General Assembly on September 19, 2017, “today's World Youth is the largest generation in the history of all mankind in terms of number, since they are 2 billion people. The next day of the planet, the well-being is associated with how our children grow up as human beings. Our main task is to create the necessary conditions for youth to show their potential, to prevent the spread of the “virus” of the idea of violence. To do this, it is necessary to develop multilateral cooperation in social support of the younger generation, protection of its rights and interests. So, in this, first of all, the formation of the consciousness thinking of young people on the basis of enlightenment is the most important task" [1], it has been established that their emphasis is a priority.

Due to the growing popularity and coverage of internet cafes on the streets with the Internet and mobile internet, the market is practically absent and the access of minors to the internet has been restricted. The situation of uncontrolled and prolonged teenagers in Internet cafes has also improved significantly. It can be said that Uzbek youth have entered the mature stage of access to the Internet. They learn that today's Internet is a huge encyclopedia. After all, the internet has gradually evolved from a children's toy platform to a tool platform for children's reading, life and entertainment. With the advent of the Internet era, many concepts and models of traditional society undergo revolutionary changes, and today's teenagers become the internet “creator” of tomorrow.

With the efforts of schools and families, teenagers realized that the internet space contained horror, violence and unhealthy things, just like in real society. If adolescents cannot consciously increase their consciousness on prevention, unhealthy things poison them directly or indirectly. This type of problem has long become the focus and hotspot of parents, schools and the community as a whole. The survey showed that most teenagers had a simple and straightforward understanding of the disadvantages of the internet. They know that sitting online for a long time affects their vision, know that they need to be wary of bad content and bad friends, and know that there is a lot of time to work on the internet. Such entertainment affects their studies. But when asked about the deeper problems of network security, most children are not very clear or react indifferent. In our opinion, current teenagers are very intelligent. They have basic abilities such as understanding physical things correctly, separating the right from the wrong.

Teachers and parents are healthy and intelligent when they are properly guided, students remind each other, and they strengthen communication and control. With the acceleration of the construction of “digital cities” and “smart cities” in our country, “Smart Education” is introduced into the agenda, schools, students, families and the educational e-commerce industry become more and more dependent on the internet. "Smart cities “assumes community participation as a whole, and” smart education" assumes a wide range of adolescent participation. The widespread use of the internet by adolescents becomes a common phenomenon. Therefore, it is relevant to ensure Internet education and network security for young people. According to A.U.Anorboyev, “the head of the Russian section of the International Police Association, Lieutenant General Yuri Zhdanov, estimates that the number of cybercrime in the world increased by 71.4 percent in 2020 compared to 2019. As a result of the reforms carried out by the states in this regard, there are currently more than 500 legislative acts on Information protection, Information disclosure, computer crime, and in Uzbekistan, separate legislative acts that regulate this have not been developed to the proper level and, taking into account the following circumstances, create a safe cyberspace in our country the need to define the relationship to the extent necessary is emphasized” [2].

Network security for teenagers mainly includes general concepts such as not seeing unhealthy content, setting passwords for accounts, and installing anti-virus programs. In fact, Network Security has a long history of development.

After the advent of radio engineering, password telegraphy appeared; after the advent of computers, security measures such as user accounts and passwords, control over the use of permissions were introduced into the operating system; after the appearance of local networks, protocol security measures reliability, file servers and personal computer terminal DOS operating system security measures and virus scanning software appeared, after the appearance of the internet, security measures to ensure the safety, integrity and availability of information and information systems continue to mature, and the information security system is gradually improved, The widespread use of TCP/IP networking computers in the early days of computers made it possible to fully interconnect the three main areas of application of scientific computing, automatic control, communication and information processing and become a cloud computing platform. Facilities, industrial control system facilities (ICS) and communications and objects of Information Systems. Technologies, equipment, and equipment in these three main areas were closely linked, and security risks and threats also began to affect each other.

The concept of information security and its meaning and expansion once again intensified, giving birth to new technologies. Cyberspace (cyberspace, network space, cyberspace) theory, cyberspace has become the fifth largest area of activity for humanity after land, sea, air and space. Like other spaces, the issue of Cyberspace Security (referred to as network security) is very prominent. The various levels of confrontation between network infraction and defense have been very intense, and network security has become a hot spot in the world's spotlight. Information technology of the president of the Republic of Uzbekistan dated September 14, 2019 and on additional measures to control the introduction of communications, to improve the system of their protection”

According to resolution PQ–4452, the Center for cybersecurity has conducted 114 website examinations by the DUK throughout 2020 to June 25, 2020, 253 national uz domain areas have identified information security incidents, 58 government organizations have identified information security[7].

Countries around the world have changed their network security strategies and upgraded network security to a level that affects national security. Some states divide network security into national security and Public Security. National security in terms of network security and public safety is closely related, but has different meanings. Therefore, N.Salayev and R.Roziyev calls the illegal dangerous act committed directly through computer tools or by means of storage technologies in the field of Information Technology, referring to information technologies as references, to which computer crime is synonymous. Also, a computer system, a network, as well as other tools that can be accessed or with the help of a co-computer system, a network or in a cyber environment against computer information the committed socially dangerous act is described as cybercrime, definition of the above crimes as a different crime from cybercrime give[3].

Documents related to foreign countries (North America, the European Union, NATO, etc.) reflect clear content definitions of national security and Public Security and differentiated security measures. National security and the important difference between public safety lies in the "audience", just as in some products there are differences between "military" and "civilian", "special purpose" and "general use". When general-purpose goods are simply applied in special security parts of a national critical information infrastructure, the lack of a “one-dimensional” and individualistic security model leads to different levels of consequences. Therefore, "cybercrime can be classified into two groups based on which space the socially dangerous act is committed, namely cybercrime committed in cyberspace belonging to the information and communication technology sector and cybercrime committed in the information sector. Both crimes are committed in cyberspace, but in cyberspace in information and Communication Technology, Information and communication technology can be damaged or brought to a state of harm. In cybercrime in the information sector, however, information and communication technologies are not harmed, but the interests of the individual, society and the state are undermined by the fact that information that harms users is stored, transmitted and used in their information and Communication Technology. Depending on the occurrence of cybercrime in relation to the object, it is divided into cybercrime directed against the life, health, morality, rights and interests of the individual, socio-political, economic, information and communication technologies."[2].

National security requires special and military technologies to ensure public safety, common technologies and civil products can be used to prevent public safety. Network security includes a wide range of content and coverage. Wherever information technology develops, it can be said that network security issues also accompany it. It is difficult for adolescents to fully understand this and unlikely to fully understand it. For this reason, young students are advised to first establish a hierarchical view of network security in the study of network security knowledge.

For most young students: first, it is necessary to establish basic concepts of network security, raise awareness of network security and establish awareness of national network sovereignty, data sovereignty and the preservation of personal privacy rights. Physical growth and they must follow the instructions of the school and parents. Requirements: should develop good Internet habits, use the Internet to a limited extent and reject unhealthy information. The second is an additional understanding of the relevant knowledge of General network security and the acquisition of General network security skills, for example: learning to independently adjust the security settings of computers and other equipment, solving common network failures and security problems, preventing common network threats, and actively supporting the green network environment in the fight against disruptive behavior on the internet is important.

Therefore, relevant educational departments and schools in our country offer knowledge courses in Information Technology and network security based on real conditions. For young people with experience in information technology, they can learn more and master the deeper content of Information Technology and network security technology so that they become young professionals in network technology and network security technology and become good seeds. In the opinion of O.G. Davlatov, "ensuring information security requires, first of all, the analysis of information from various sources of Information, assessment and identification of harmful information, the preparation of students to protect themselves and members of society from the threat of harmful information, to fight them"[5].

There are so-called very powerful "small hackers" groups in the country and abroad. In fact, these "little hackers" are primarily very interested in the Internet, and the logic of persistent traditional and positive thinking in the study of network technology, they are often called Network "players" who come up with fantastic and genius ideas and reverse logic, and at the same time show operational skill and confidence. In our eyes, of course, the most pressing issue today is to teach such talented young people from an early age to properly look at the safety of the network, love for the motherland, compliance with the law.

The Internet is an open network environment. Everything in the world develops in a certain state of balance. If this balance is disturbed, problems arise and disasters occur. The same applies to the development of the internet. The opposition between “openness” and “restraint” should adopt a relatively balanced strategy to some extent. If openness is done blindly, events similar to “WikiLeaks” also occur. In this regard, on the one hand, the countries of the world are actively promoting interaction with an open attitude in the process of developing the Internet, on the other hand, they have developed relevant laws, rules and rules of behavior to limit openness. Because the biggest problem that “openness” brings is that “harmful things” also enter people's activities with openness, harming the interests of users, poisoning young people. To this end, governments around the world filter access to certain data content on the internet to prevent the spread of harmful information in accordance with the concept of protecting their own interests and perception and began to limit. Therefore, in the United States, Computer Crime losses have reached trillions of dollars, and annual losses are ten billion dollars. The Federal Republic of Germany loses US $ 9.5 billion each year. In the UK, this pointer is worth US $ 2.5 billion.

There is a computer fraud in 40 seconds. The problem of ensuring information security in Asia is also very serious, such as Japan and Singapore where tens of thousands of people have publicly reported computer crimes[6].

Conclusions

The chaotic opening of virtual internet, such as the real physical world, allows a variety of malicious content to influence people's opinions and activities. Criminals use the internet to steal other people's bank deposits, sell personal information, create and spread false news. As you can see, managing the Internet is essential. Relevant departments are advised to strengthen internet remediation work in the following areas to create a green and environmentally friendly internet environment for young people:

1. Promulgation of laws and regulations related to Internet governance. National Security Act, Cyber Security Act and accelerate the improvement of relevant laws and regulations, such as cybersecurity verification measures, and study and formulate a code of ethics for young people to use the Internet.

2. Adoption of scientific strategies and concepts of internet management. Manage all sorts of irregularities on the internet. In competition between enterprises, the use of the internet network to carry out cyber attacks of various forms is prohibited; the use

of telecommunication resources for sending spam text messages, telecommunications fraud and illegal sale of confidential data of customers is prohibited; disclosure of security vulnerabilities is prohibited. Important national information systems on the internet; it is forbidden by individuals to scan for vulnerabilities and detect attacks on important national Information Systems, and to carry out unorganized attacks on others.

3. Creating a special area and column for the youth of the Internet. Children
and providing "network protection" for elementary school students and healthy and child-friendly Internet information websites and government guidance to logically link the lines allocated to the school and the use of market methods such as corporate participation and even the creation of a National Education Cloud Platform to collect educational data.

4.Internet management internet operators, equipment vendors and the formation of the framework of the corporate environmental alliance from other service companies, the fulfillment of corporate obligations on security, the product and ensuring the safety of services requires the provision of guarantees for the safe travel of young people on the internet.

5. Speed up the management of Smart terminal APP applications. The number of Android APP apps for smart phones in our country is amazing and security issues are very important. To create an app review and evaluation mechanism to change the decisive problems of APP application security.

To make the dream of becoming a powerful state with the internet come true, we need to start educating young people from the stage of “childhood”. Government and enterprises should create conditions for young people to use the Internet, direct them to active innovation, use their talent. The development of Future "Smart Cities", e-commerce and internet technologies, it is necessary to join the ranks of the world's cyber security forces as soon as possible.

REFERENCES

1. 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.;

2. Anorboyev A.U. Kiberjinoyatlarning jinoiy-huquqiy jihatlari. Doktorlik (PhD) dissertatsiyasi avtoreferati. –Toshkent, 2021. –B.13.;

3. N.S.Salayev, R.N.Ro‘ziyev. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. MonografiY., – T.: TDYUU, 2018, 139-b.;

4. Anorboyev A.U. Kiberjinoyatlarning jinoiy-huquqiy jihatlari. Doktorlik (PhD) dissertatsiyasi avtoreferati. –Toshkent, 2021. – 14-15 betlar.;

5. Davlatov O.G‘. Talabalarda axborot xavfsizligini ta’minlash kompetentligini tarixiymadaniy meros vositasida rivojlantirish. Pedagogika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi avtoreferati. –Toshkent, 2018. –B.11.;

6. Международная информационная безопасност: Теория и практика. В 3 т. (+СД) Под общ.ред А.В.Крутских Москва Аспект Пресс 2021. - 384с.

7. https://tace.uz/uz/.