Advances in Economics, Business and Management Research, volume 128
International Scientific Conference "Far East Con" (ISCFEC 2020)

Training Teenagers to Ensure Their Own Cybersecurity

E V Chernova[1], I V Gavrilova[1]

[1]Nosov Magnitogorsk State Technical University, Magnitogorsk, 4555000, Russia

E-mail: i.gavrilova@magtu.ru

Abstract. iInformatization of education and all aspects of everyday and professional life have led to the fact that modern man can not fully function outside the digital environment. The most vulnerable to the manifestation of cyberthreats and negative impacts of ICT are adolescents, due to the peculiarities of physiology and personal development. At the present stage of humanities development not enough attention is paid to the problem of teaching teenagers the basics of personal cybersecurity in the information technology use. The article presents the content of the course "Fundamentals of cybersecurity" for children of early adolescence, developed on the basis of the personal cybersecurity needs analysis from modern ICT-threats.

1. Introduction

Personal computers, tablets, mobile phones and other gadgets, social networks, cloud storage, Internet education, electronic journals and diaries – all this is a confirmation that modern technology has become an integral part of our lives. A rare person can do in everyday life without the amenities provided by information technology and devices. It is obvious that such a symbiosis of human and ICT gives both positive results and a number of negative consequences. One of the relatively new challenges posed by ICT and the development of the information society is the problem of human information security, in particular the information security of the child.

In the Internet, and not only, there are many hidden and obvious threats, and if adults because of their life experience are still able to resist the most common and obvious, the child is most vulnerable to information and cyber threats. Most of today's children can not live a day without the Internet and gadgets, almost all the activities of the child is mediated by the use of ICT. However, the skill of using ICT capabilities to solve everyday, educational and communication tasks does not automatically mean the skill of ensuring one's own cybersecurity. Stealing accounts, phishing, bullying online (cyberbullying), deadly games, inappropriate content, suspicious travelers, a waste of parents ' money, viruses are just some experiences of students in the Internet.

Modern education stimulates the use of ICT in the educational child activities, technologies are included in both educational and extracurricular activities. Entertainment activities of children today is also in the plane of information technology. There is a problem of children unwillingness to provide their own personal security in the information space. The earlier a child gets into the ICT environment, the more vulnerable he / she is to the impact of cyber threats, as there is no life experience and knowledge that will allow him / her to identify the threat and competently prevent it or resolve the situation with minimal losses [1].

2. Cyberthreats and cybersecurity of children in early adolescence

"According to the UNFPA terminology of the United Nations population fund, adolescents are persons aged 10-19 years, with the early adolescence being the period from 10 to 14 years" [2]. This age is characterized by a period of active knowledge and formation of the teenager personality, if the child is ready to obey the authority of an adult, the teenager is already seeking to learn the truth only through his own experience. Trying to protect themselves from the influence of adults, the teenager often commits acts that can lead to undesirable consequences. Curiosity, openness, lack of experience – makes it easy prey for criminals.

Consider modern cyber threats specific to a teenager 10-14 years.

According to our research, the first place is the problem of unwanted information availability – information that does not correspond to the age of the child, causing harm to the psyche and health, violating legal requirements.

Further, it should be noted the formation of deviant behavior in the field of ICT – "a kind of an individual (a group of individuals) deviant behavior, representing a system of actions (or individual actions), mediated by the use of ICT (or aimed at ICT), causing damage (moral, physical, economic and other) to society, organizations, individuals or the individual" [3]. Among teenagers this behavior most often manifests itself in the form of trolling, dependence from computer games, cyber hooliganism and other.

Of special note is the problem of adolescents engaging in suicidal and deadly game. In 2016, Russia has identified a network cybersuicide games "Blue whale". The organizers of this game were selected by teenagers with the help of a number of jobs, which screen out children with a healthy psyche and normal behavior. Children who performed tasks and passed to the next level were intimidated by the consequences of leaving the game. The tasks included-inflicted wounds and injuries, sometimes animal abuse and minor peers, and so on. The purpose of the curator was – to bring the child to victory – suicide. The game stopped after arrest one of the leaders, as well as the blocking of all communities, which at least remotely resembled the meaning of the community game. Today in Russia among older adolescents is gaining popularity game "24", the meaning of which – for 24 hours gap from the field of the parents view and not to tell how or where you were these days. For teenagers and younger children there are "adrenaline games" – to cross the road in front of the car, who will stand longer in front of the train, etc. Unfortunately, most of these games adults learn about after the first victims – the rules of the games are distributed in closed communities, children are forced or persuaded to maintain secrecy.

The problem of cyberbullying is acute all over the world. Children's age, the aggressiveness is a breeding ground for cruelty and persecution of their peers. The lack of self-criticism, empathy pushes children to pursue the victim "for fun", most of the bullying moved to a more comfortable virtual environment. Victims of bullying are often afraid to report harassment to adults, or do not find the response and assistance, as not all parents are willing to understand the seriousness of the situation and to find adequate instruments to address the cyberbullying problem.

Leakage, loss of personal information, disclosure of teenager confidential information is one of the threats to cybersecurity. Not every adult is ready to accept the loss of important information. What to say about a teenager who is at a special age. The first question at the master classes that we hold for students: and teach us to hack social networks.

We have found that the current state of education does not take into account the state of the information environment development [4], training programs designed for early adolescence, do not implement the prevention of the cyber implementation, do not provide the teenager with the skills to ensure personal cybersecurity when using information and communication technologies.

3. Teaching teens cybersecurity

We studied the main cyberthreats and problems of early adolescence children cybersecurity, and on the basis of this developed a methodology for the formation of skills to ensure the personal cybersecurity of adolescents. This technique is proposed for use in the system of a teenager additional

education, as we understand that its rapid implementation in the state educational programs is difficult due to objective reasons. The biggest challenge of learning the cybersecurity basics is the rapid change of the surrounding information space.

Our team has developed a number of teaching materials aimed at helping teachers and covering the main aspects of the adolescent cybersecurity problem in the modern information space [4-14].

So, what should teens learn in order to build personal cybersecurity skills:

- Improving technical literacy.
- Knowledge of the main cyberthreats, their characteristics, forms of manifestation, methods of prevention and deactivation.
- Ways to preserve physical health during long-term work with ICT-devices.
- Ways to preserve mental health in IR-space.
- Training in the implementation of payments on the Internet, fraud detection, safe behavior.
- Learning Netiquette, responsibility for your words and actions on the Internet.
- Practicing safe behavior in the cyberthreats event.

Negativism of teenagers, instability of their mentality put forward special requirements to forms of the educational activity organization. The current generation of students is very different from previous generations. So, it is necessary to change approaches to their training. It is offered "to use active training methods, to increase the educational process interactivity, to apply the gamification principles» [15]. We developed our methodology using gamification technology and incorporating ICT-tools into the process.

Gamification is a way of organizing educational or professional activities with the help of gaming technologies, including those based on computer games. The gamification principle implies the introduction into the educational process of elements from other areas (games, social networks) to create a more convenient and attractive educational environment.

The scope of gamification can be any complex and routine activity, the content of which causes the subject to decrease motivation. It distracts attention from the monotony by setting the user one or more interesting tasks, the implementation of which can improve the skills provided by the educational program. The aim of gamification is "to change the usual behavior of the audience, involvement in activities, the content of which remains the same, but in a certain way is processed to increase motivation to solve the problem, as well as to increase the time that the student devotes to solving it» [16]. However, gamification in itself "cannot be a key to improve the level of students training. This is nothing more than an auxiliary element. However, it is a tool that, if used correctly, will increase the motivation and involvement of students in the educational process» [16].

The principal difference between gamification and the previously known educational game forms is the absence of virtual reality substitution, which reduces the risk of deviant behavior, because there is no one of the main factors of dependence on computer games formation: the departure from reality. A gamified educational course is not a computer game, even if it has a special virtual environment with a good game design. When moving along the trajectory of the course, the student performs educational and game tasks. For example, in our course, a teenager is trained at the school of defense against the dark arts under the guidance of the director Dragomira Putyatishna Bayun. The Director is a nod to the slavic history and mythology: cat Bayun – fabulous cat-eater, fascinating travellers with her magical voice if the traveler is not ready to oppose him, the cat kills him. In general, the course uses other interdisciplinary connections, as the course is aimed at forming a holistic picture of the world, when cybersecurity is one of the real-world components, not a miracle, but the norm of behavior in the teenager modern information reality.

At the same educational goals always remain the priority, and the game is designed to encourage the preservation of intrinsic motivation to educational tasks performance.

4. The "Fundamentals of Cybersecurity" course

The purpose of the training program "Fundamentals of cybersecurity" – the formation of skills and safe abilities and appropriate behavior when working with computer programs and the Internet, the

ability to comply with the rules of information ethics and law, use ICT-tools in solving cognitive, communicative and organizational problems in compliance with the requirements of ergonomics, safety, resource conservation, information security, understanding the basics of the legal computer programs and the Internet use aspects, etc.

As a result of the program development, the student must acquire the following knowledge and skills:

know:

- information ethics and Netiquette standards;
- threats to personal and information security in the modern information space;
- the legal basis for the placing and information use in virtual space;
- safety standards of physical health when working with information devices;
- ways to protect the individual with negative information effects;
- ways to save information on devices (leakage, loss, backup, archiving, encryption, etc.);
- ways to promote yourself, your projects on the Internet, using legal tools.

be able to:

- create and set up accounts on any electronic resources, taking into account age, ethics and law;
- create unique and hard-to-crack passwords;
- configure mobile devices in accordance with the requirements of personal security (surveillance, access, information security, information transfer, etc.);
- install and configure software for information devices (licensed and free software, verified data sources, etc.);
- use built-in and additional tools to ensure information security on devices;
- use any type of media safely;
- work safely on other people's devices;
- use information from any source without copyright infringement;
- determine the reliability of information from different sources.

This course is designed for middle school students. The complexity of training is 100 hours (including 26 hours of lectures, 69 hours of practical training, 5 hours – intermediate control and certification).

5. Conclusion

Summarizing the above, we can state with confidence that the problem of ensuring personal cybersecurity for adolescents is currently very important, but it is quite difficult to solve it by means of general school education. The specifics of information security is such that threats and security solutions are changing simultaneously with the development of technologies and the implementation of individual IT-solutions. However, the proposed methodology can be taken into account in the development of educational standards in computer science, despite the fact that it was developed for additional education.

References

[1] Chernova E V, Dokolin A S, Gavrilova I V 2018 Formation in early adolescence of readiness to ensure personal cybersecurity *Computer science and education* **7 (296)** pp 16-25

[2] Chernova E V and Gavrilova I V 2018 Developing a willingness to provide personal cybersecurity in early adolescence *The international science and technology conference «FarEastCon»* pp 752-759

[3] Zerkina E V and Chusavitina G N 2008 Future teachers preparation for the prevention of students deviant behavior in the information and communication technologies field (Magnitogorsk, MaGU) pp 5-180

[4] Chernova E V 2019 The problem of systematic teaching students the basics of cybersecurity *Abstracts of the 77th international scientific and technical conference "Actual problems of modern science, technology and education"* pp 446-447

[5] Chernova E V 2015 Innovative educational technologies in teaching the basics of information security *Electrotechnical systems and complexes* **1 (26)** pp 52-55
[6] Chernova E V and Dokolin A S 2016 The development of cyber extremism in the youth environment *Modern problems of fundamental and applied sciences development materials of the II international scientific-practical conference* pp 104-108
[7] Dokolin A S 2017 Formation of university students' readiness to counteract involvement in cyber-extremist activities. *Doct. Diss.* (Belgorod) pp 3-20
[8] Dokolin A S and Chernova E V 2015 Project method in the prevention of youth involvement in cyber extremism activity *SworldJournal* **8** pp 25-31
[9] Efimova I Iu and Varfolomeeva T N 2015 The role of parents in ensuring the information security of students when using the Internet *Information security and prevention of cyber-extremism among young people Materials of the intra-University conference* pp 205-218
[10] Chusavitina G N and Karmanova E V 2018 The use of web 2.0 network services in the implementation of the project approach in information security training *Computer science and education* **4 (293)** pp 27-36
[11] Karmanova E V and Turkova E S 2013 Methodology of web-seminar on "Information security" for high school students *Information security and prevention of cyberextremism among young people* pp 56-61
[12] Karmanova E V and Chernova E V 2018 Experience in using web 2.0 services to prevent the involvement of students in cyberextremist activities *Materials of the scientific-practical conference "Management mechanisms to counter the ideology of extremism and terrorism"* pp 94-98
[13] Romanova M V and Chernova E V 2017 Methods of organization of extracurricular activities in Informatics and ICT (Magnitogorsk, Izd-vo Magnitogorsk. gos. tekhn. un-ta im. G I Nosova) pp 5-212
[14] Movchan I N, Chernova E V, Chusavitina G N 2015 Educational project as one of the forms of counteraction to cyberextremism among schoolchildren *Fundamental study* **9-3** pp 486-490
[15] Karmanova E V 2018 The use of gamification in the organization of e-learning (on the example of the training course "Information systems and technologies») *Actual problems of modern science, technology and education: abstracts of the 76th international scientific and technical conference* vol 2 p 45
[16] Kurzaeva L V and Gavrilova I V 2018 Methods of implementation of mass open online courses in the educational process (Magnitogorsk, Izd-vo MGTU im. G.I. Nosova) p 35