Forum: Special Conference

Issue: Protecting Children from the Dangers of the Internet

Student officer: Alisa Balybina

Introduction

Internet is a global information network. Its parts are connected with each other through a single address space based on the Internet Protocol. The Internet consists of many computer networks and provides remote access to computers, e-mail, message boards, databases and discussion groups. The existence of the Internet gives access to a huge amount of information, some of which can harm people both mentally and financially. The Internet is a space for criminals willing to harm people of all ages. Children are the most vulnerable part of the population because their worldview is not yet formed.

According to statistics, the Internet is used by 4 billion people, it is a half of the inhabitants of the Earth. That is why the issue of protecting people from online dangers is so momentous.

The most harmful acts in the Internet space can be:

• suicide sites;

• sites forums potential suicide;

• drug sites (the Internet is full of news about the "benefits" of marijuana, recipes and tips for making potions)

• sites inciting ethnic strife and racial rejection (extremism, nationalism, fascism);

• pornographic sites;

• dating sites (virtual communication destroys the ability to real communication that causes the loss of communication skills among children; it can also be dangerous as it is possible for criminals to deceive children);

• websites promoting extremism, violence and deviant behavior, direct threats to the life and health of schoolchildren from strangers offering personal meetings, as well as various types of fraud;

• sects (virtual interlocutor can affect the outlook of a child).

Children use the Internet for communication, entertainment and learning. There is a tendency for children to start using websites at an earlier age. Therefore, it is necessary to make this use as safe as possible in modern society.

Definition of key terms

Cyber abuse – online behavior which is reasonably likely to have a seriously threatening, intimidating, harassing, or humiliating effect on a person. It is such a behavior that threatens to hurt a person socially, psychologically, or even physically.

Cyberbullying can occur in many ways, including:
* abusive texts and emails
* hurtful messages, images or videos
* imitating others online
* excluding others online
* humiliating others online

Image-based abuse (IBA) occurs when intimate, nude or sexual images are distributed without the consent of those pictured.

Social engineering – the act of manipulating people into performing actions or divulging confidential information like passwords and PINs.

Child – a human being between the stages of birth and puberty.

Background information

The ideas about the need and benefits of combining all computers into a network visited the best minds in the middle of the XX century. In 1962, his views on the problem were expressed by John Licklider from Massachusetts Institute of Technology (USA). In his works you can find bold predictions for the near future, concerning the creation of a global network of computers from different parts of the world, where each user has access to information of interest to him. The first network, which united only 4 computers, was called ARPANet. The main task was to provide communication between military and educational institutions in the case of the Third World War. In 1996, there already were about 300 nodes, and tens of thousands of subscribers got access to the virtual space. Today, the Internet unites millions of office and home computers, gives huge possibilities for self-expression, communication, information search work, and entertainment.

1) Current situation

Analytical Agency *We Are Social* and the largest SMM-platform *Hootsuite* jointly prepared a package of reports on the Global digital market 2018. According to these reports, more than 4 billion people around the world use the Internet today.

More than half of the world's population is online now, and about a quarter of a billion of them went online for the first time in 2017. Africa has the fastest growth rate — the number of Internet users on the continent has increased by more than 20% compared to the same period last year.

Key factors in the growth of the Internet audience these last years are affordable smartphones and cheap tariffs for mobile Internet. In 2017, more than 200 million people became owners of mobile devices for the first time, and now two-thirds of the world's 7.6 billion people have a mobile phone.

More than half of today's mobile devices are classified as "smart", so it is becoming easier for people to access all the features that the Internet offers, wherever they are.

The growth is also noted in the audience of social networks. In the last 12 months, the number of people on the most popular social platforms has been increasing daily by almost 1 million new users. Every month more than 3 billion people interact with social networks, and 9 out of 10 go there from mobile devices.

The main conclusions of the reports are discussed in detail below, and for now-here is a brief overview of the most important metrics in the field of digital in 2018:

- The number of Internet users in 2018 reached 4,021 billion people, which is 7% more than in the same period last year.
- The audience of social networks in 2018 totals 3,196 billion people-plus 13% to last year's figure.
- In 2018, 5,135 billion people use mobile phones-4% more than a year ago.

2) Children and Internet

As can be seen from these reports, Internet is becoming more and more popular and more easily accessed. This means, that it is also easily accessed by children, and this can cause a lot of dangers. Nowadays even students of primary school usually have their own personal smartphone with Internet access, and often children’s parents do not control which content their child has access to.

While being in danger themselves, children may also unwittingly expose their families to online risks, for example, by accidentally downloading malware that could give

cybercriminals access to their parents' bank account or other sensitive information. According to Kaspersky antivirus website, the greatest risks children face online are the following:

1. *Cyberbullying*

   According to Internetsafety101.org, 90 percent of teens who participate in social media have ignored bullying they've witnessed, and one third have been victims of cyberbullying themselves. Social media and online games are today's virtual playground, and that is where much cyberbullying takes place.

2. *Cyberpredators*

   They can stalk kids on the Internet, taking advantage of children's innocence, abusing their trust and, perhaps, ultimately luring them into very dangerous personal encounters.

3. *Posting Private Information*

   Children do not yet understand social boundaries. They may post personal information online, for example in their social media profiles that should not be out in public. This might be anything from images of awkward personal moments to their home addresses.

4. *Phishing*

   Phishing is what cybersecurity professionals call the use of emails that try to trick people into clicking on malicious links or attachments. ("Hey—thought you might like this!") This can also be done with malicious text messages (then it's called "smishing").

5. *Falling for Scams*

   Children might fall for scams that offer things they may prize, such as free access to online games. Young people are easy marks for scams because they have not yet learned to be wary. As with phishing, cybercriminals can use sites popular with children to identify potential victims, and then promise them something in turn for what they want—like parents' credit card information.

6. *Accidentally Downloading Malware*

   Malware is computer software that is installed without the knowledge of permission of the victim and performs harmful actions on the computer. This includes stealing personal information from your computer or hijacking it for use in a "botnet," which causes sluggish performance. Cybercriminals often trick people into downloading malware. Phishing is one such trick, but there are others—such as convincing victims to download purported games—that can be especially beguiling to children.

Relevant treaties and UN resolutions

Legislation on cyberstalking varies from country to country. Cyberstalking and cyberbullying are relatively new phenomena, but that does not mean that crimes committed through the network are not punishable under legislation drafted for that purpose.

There are several levels of legal regulation of relations emerging in the Internet:

- international;
- regional (within the European Union and CIS);
- national.

Key acts adopted in the last ten years:

- UN international trade law
- The model law on electronic Commerce 1996. (with additional article 5 bis adopted in 1998.);
- The model law "On electronic signatures" 2001.

By The Council of Europe:

- Convention on the protection of individuals with regard to the automatic processing of personal data of 28 January 1981. (Strasbourg);
- Additional Protocol to the Convention on the protection of individuals with regard to automatic processing of personal data concerning Supervisory authorities and cross-border data flows of 8 November 2001. (Strasbourg);
- Convention on information and legal cooperation concerning the "services of the information society" of 4 October 2001;
- Council of Europe Convention on cybercrime of 23 December 2001.

The International Chamber of Commerce:

- A common practice for certified digital and international Commerce 1997;
- General principles of advertising and marketing on the Internet 1998.

Possible solutions

The problem of protecting children from Internet dangers may be dealt with on several levels:

1) At home level:

- Create a list of home rules for visiting the Internet with the participation of teenagers and demand its unconditional implementation. Specify the list of prohibited sites ("black list"), Internet hours, guide to communicate on the Internet (including chat rooms).
- Discuss children's friends on the Internet they communicate with through instant messaging services to make sure they know them in real life.
- Use tools to block unwanted content as a Supplement to the standard Parental controls.
- Encourage the use of moderated chats
- Insist that children should never meet Internet friends in real life
- Encourage children not to give out personal information through email, chat, instant messaging, registration forms, personal profiles, or when registering for online contests.
- Instruct children not to download programs without your permission
- Encourage a child to report any threats or concerns related to the Internet
- Set a password so that personal information does not get to strangers

This information may be delivered to children by their parents and/or school teachers. However, parents as well as teachers need to get these instructions that will be developed by professionals on a country or international level.

2) At national and international levels

- Developing guidelines for schools and parents with the information listed in the previous point
- Strengthen national and international measures to prevent cyber crimes
- Establish legal liability in all countries with Internet access