Zhytomyr Ivan Franko State University Journal. Pedagogical Sciences. Vol. 3 (98)

Вісник Житомирського державного університету імені Івана Франка. Педагогічні науки. Вип. 3 (98)

ISSN (Print): 2663-6387
ISSN (Online): 2664-0155

UDC 004.738.5.056. - 053.5:070(073)(045)
DOI 10.35433/pedagogy.3 (98).2019.69-77

ONLINE RISKS AND INFORMATION PROTECTION OF CHILDREN ON THE PAGES OF PEDAGOGICAL PRESS OF THE USA

A. S. Paukova*

The Internet is the most popular mass media among young people. It not only provides children with powerful learning and entertainment opportunities, but it is also an environment where they can face many risks. That is why the problem of information protection of children, especially online safety, is one of the priority areas for the development of pedagogy and education not only in the USA but also in Ukraine. Publications array focusing on the main methods and tools for overcoming online risks has been analyzed. The article deals with the main types and classifications of online risks: content risks, communication risks, electronic risks and cyberbullying. Cyberbullying classification is provided: trolling, harassment, impersonation, denigration, happy slaping, fraud, online alienation, sexting and cybergrooming. The author highlights American legislation on child protection on the Internet. The strategies for implementing the above legislation into the American School System are described.

The main strategies of information protection of children are identified and analyzed: media literacy, critical thinking, awareness of parents, children and teachers about online risks, adherence to the rules of online behavior. The terms media literacy, media education and critical thinking are revealed. The article provides criteria for evaluating online resources that help children effectively analyze, comprehend, and critically select information. Issues of content, source and data evaluation, site structure that develop critical skills for evaluating an online resource are described. The author defines and analyzes the main tasks of lessons for the formation of information protection of children on the Internet. The basic knowledge and skills that children need to have for working safely on the Internet are identified.

Key words: *the Internet, risks of the Internet usage, social networks, media literacy, media education, critical thinking, information protection, evaluation and selection of information, control technologies, unacceptable content.*

* Postgraduate Student
(Luhansk Taras Shevchenko National University, Starobilsk)
alinusua@gmail.com
ORCID: 0000-0002-6392-883X

РИЗИКИ ТА ІНФОРМАЦІЙНИЙ ЗАХИСТ ДІТЕЙ В ІНТЕРНЕТІ НА СТОРІНКАХ ПЕДАГОГІЧНОЇ ПРЕСИ США

А. С. Паукова

Інтернет є найпопулярнішим засобом масової інформації серед молоді. Інтернет надає дітям потужні можливості для навчання та розваг, але також є середовищем, де вони можуть зіткнутися з багатьма ризиками. Ось чому проблема інформаційного захисту дітей, особливо безпека в Інтернеті, є одним із пріоритетних напрямків розвитку педагогіки та освіти не лише у США, а й в Україні. Проаналізовано масив публікацій, присвячений основним методам та інструментам подолання онлайн-ризиків. У статті розглядаються основні типи та класифікації ризиків в Інтернеті: контентні, комунікаційні, електронні та кібербулінг. Надається класифікація кібербулінгу: тролінг, домагання, наклепи, самозванство, хепі слепінг, ошуканство, онлайн відчудження, секстінг та кібергрумінг. Автор висвітлює американське законодавство щодо захисту дітей в Інтернеті: "Акт про Захист Прав Дітей у мережі Інтернет" (CIPA)) та "Про захист дитячої конфіденційності в Інтернеті" (COPPA)).

Описуються стратегії втілення вищезазначених законодавчих актів в Американську шкільну систему. Визначено та проаналізовано основні стратегії інформаційного захисту дітей: медіаграмотність, критичне мислення, обізнаність батьків, дітей та вчителів про ризики в Інтернеті, дотримання правил поведінки в Інтернеті. Розкриваються терміни медіаграмотність, медіаосвіта, критичне мислення. У статті наведено критерії оцінювання Інтернет-ресурсів, які допомагають дітям ефективно аналізувати, осмислювати та критично відбирати інформацію. Описані питання контенту, оцінювання джерел та даних, структуру сайту, що розвиває критичні навички оцінювання Інтернет-ресурсу. Автор визначає та аналізує основні завдання уроків формування інформаційного захисту дітей в Інтернеті. Визначено основні знання та навички, які повинні мати діти для безпечної роботи в Інтернеті.

Ключові слова: *Інтернет, ризики та небезпеки мережі Інтернет, соціальні мережі, медіаосвіта, медіаграмотність, критичне мислення, інформаційний захист, оцінювання і відбір інформації, технології контролю, небажаний контент.*

Introduction of the issue. Nowdays, the Internet is the most popular mass medium especially among young people. The Internet offers the user great opportunities as a high-tech source of communication for searching and receiving information. With the rapid development of the Internet it has become a special kind of reality – virtual reality, which is not only the means of communication, but it is also an information and entertainment resource. Through the Internet, children and teens discover the world around them, form their own personality.

The outline of unresolved issues brought up in the article. The problem of information protection of children, especially online safety, is becoming a priority in the development of American pedagogy and education. This problem is revealed on the pages of the American pedagogical press. The authors of articles emphasize that informing children, educators and parents about the main risks and dangers of the Internet is one of the main ways of information protection of children. A lot of articles are devoted to the analysis and classification of online risks. Most of the articles describe methods, strategies for overcoming risks of the Internet usage and the technologies of parental control. Other researchers cover the topic in such ways as information literacy, media literacy and media education of children, parents, and teachers. Therefore, in this article we have

analyzed an array of publications that focuses on protecting children from major risks and dangers on the Internet. In our opinion, such analysis facilitates the development and implementation of more effective means of information protection of children in Ukraine.

Current state of the issue. A lot of publications of scientists from different countries of the world are devoted to the issues identified: N. Willard, A. Giddens, A. James, J. Cantor, D. Kunkel, N. Crowder, S. Livingstone, J. Patchin, S. Pepper, R. Riley, V. Skinner, L. Haddon, S. Hinduja, J. Frechette who highlight the major online risks and dangers and various strategies for protecting children in their publications.

Aim of research is to review and analyze the major risks of the Internet; methods, principles, content, tools and forms of information protection of children in the USA.

Results and discussion. The large amount of information and its uncontrolled consumption in the virtual space increases the risk for children to face online dangers. The information space is especially hazardous for children and teenagers who are the most vulnerable group of the Internet users. New opportunities of the Internet network can lead to such dangers for children as harassment, blackmailing, aggression, pornography, encounters fraud and other negative content. Internet for children and teenagers has become a special social environment in virtual form. Groups, social media communities, chats, blogs, forums, games, movies, music, feelings, and relationships all move into the virtual space. In 1997, an Internet Security Summit was held in Washington. In October 1998, American President B. Clinton signed into law "Children's Internet Protection Act" (CIPA), which protects children from sexual and other unacceptable material on the Internet. Congress introduced this law only in 2000, and approved several additional acts requiring schools to take measures to ensure children's online safety. The law states that libraries and schools participating in the federal Internet access program are required to install software filters on their computers. These filters block the sites with unacceptable content [1]. According to statistics, 74 % of US schools use content filters. 59 % of parents in the USA discuss online safety rules with their children and use content filters and antivirus software [10: 1]. Schools should provide children with rules of online behavior, including interaction on social networking sites and chat rooms. Compliance with these rules is a prerequisite for obtaining federal funding. In 2004, American government allocated 9 million dollars for a program "implementation of content filters to all schools in the country" and provided a guarantee of technical support. These initiatives were later found to be imperfect. Professor J. Frechette has tested and analyzed about a dozen samples of software (Net Nanny, CyberPatrol, CyberSitter, etc.), proved that none of the censorship tilters can teach a child and adults to analyze and evaluate information in various forms outside of school and in later life [5: 558-575].

In 1988, "Children's Online Privacy Protection Act" (COPPA) was introduced and took effect only in 2000. This law regulates the collection of personal information by private and legal entities on the Internet from and about children under the age of 13 and obliges website administrators to establish and maintain reasonable procedures to protect the confidentiality, security and integrity of children's personal details. According to the law, the administrator must obtain the prior consent of parents or guardians in order to collect, use or disclose personal information obtained from children. Violation of this

law provides for liability in the form of a fine of up to one million dollars. Today, most American websites, such as Facebook, MySpace, Twitter, Second Life, the Sims, YouTube conform to the standards of (COPPA): individual must be 13 years old in order to create, manage and maintain the profile. But there are many sites for younger children without age restriction: Disney, etc [2].

However, mentioned above measures do not eliminate the problem of online risks. Most American scientists emphasize that specific software types combined with the acquisition of knowledge and skills of safe online behavior, information literacy and media education will provide effective information protection for children. According to S. Livingston, J. Patchin, S. Hinduja and N. Willard, informing children, parents and teachers about online risks and dangers is a main contributor to safe online behavior. Therefore, we consider it appropriate to identify and characterize the major threats of the Internet. Experts identify 3 groups of Internet risks:

1) content risks are materials (texts, images, audio-video files, links to third-party resources) that contain illegal, unethical and harmful information for children. For example, violence, sexual harassment (including pornography), aggressive online games, obscene language, information pertaining to racial, religious or social intolerance (extremism, terrorism, nationalism); unhealthy lifestyle advocacy (drug use, alcohol use, psychotropic substances, tobacco, anorexia, bulimia), self-harming tips (materials containing various ways of suicides); gambling, sectarianism, and material containing insults, defamation and inappropriate advertising) [4: 67-101];

2) communication risks are related to the interpersonal relationships of Internet users and include the threat of psychological attacks through e-mail, instant messaging services (WhatsApp Messenger, ICQ, Google talk, Skype etc), chats, forums, blogs, social networks, dating sites, websites (including mobile versions of these sites);

3) cyberbullying – bullying, humiliation, harassment, psychological terror aimed at causing the victim to fear or commit suicidal action[11: 492-495].

American researchers have also identified the following types of cyberbullying:

– Trolling is the placement of provocative messages with the aim of inflating the conflict atmosphere, negative reaction of users, mutual insult by violating the rules of the code of ethics of Internet interaction on the virtual communication resources [11: 496-497].

– Harassment, attacks, constant grueling attacks are repeated offensive messages directed at the victim (for example, hundreds of emails), overloading personal channels of communication [11: 498].

– Denigration is the dissemination of humiliating false information via text messages, photos, videos, songs that often have sexual content [11: 499].

– Impersonation is the process when a person positions himself as a victim by using his/her password to access an account on social networks, blogs, mail, instant messaging, or creates his/her account with a similar nickname and initiate negative communication on behalf of the victim. A feedback wave is organized when provoking victim's letters are sent to his/her friends [11: 500-504].

– Fraud, getting confidential information and disseminating it is receiving personal information and publishing it on the Internet or giving it other people [11: 505].

– Online alienation, including ostracism, isolation, social boycotting [11: 505].

– So-called "happy slapping" are any videos or photos that record real scenes of violence and then are published online [11: 506].

– Sexting is the process of sending sexual messages, personal photos using modern means of communication: email, social networks, dating sites, mobile phones [11: 507].

– Cybergrooming is a communication and establishing trust relationship with the child for a further personal meeting to have sex, physical assault, blackmailing, sexual exploitation and violence. Cybergrooming in the USA is classified as a criminal offense [10: 2-6; 11: 508-509].

Electronic (cyber) risks can be caused by malware (viruses, worms, spam attacks, spyware, bots) that can harm your computer and breach your privacy. All these malware are defined as cyber fraud[14: 40-53].

– Farming is the procedure of illegally replacing a real IP-address by the take one [14: 53-54].

– Phishing is a type of cyber fraud designed to gain access to confidential user data [14: 55].

– Sale of a non-existent product (programs, audio files, goods, information) [14: 56-57].

R. Hobbs in her scientific research emphasizes that awareness of the Internet risks partly guarantees a certain online safety for children. But the majority of American scholars believe that media literacy and media education are the most effective means of information protection of children [6: 35-38]. There are different approaches to defining the terms "media education" and "media literacy". These terms were first used in the documents of the joint meeting of the UNESCO Information Sector and the International Film and Television Council in 1973. Nowadays, in many countries the term "media education" is being replaced by a synonym for "media literacy". American researcher D. Considine notes that in the "USA today", both that terms are used almost equally, where "media education" is knowledge about the media, and "media literacy" is focused on generating critical thinking in the younger generation and protecting against negative media influences [3: 34]. R. Hobbs, one of the famous American scholars and media educators, notes in her work that media literacy can have many definitions depending on its context [7: 56]. Based on everything mentioned above, we can conclude that the main purpose of media education and media literacy is the formation of critical thinking – the process of analyzing, synthesizing and substantiating the reliability/value of information; the ability to perceive the situation globally, to find causes and alternatives; the ability to generate or change their position based on facts and arguments, correctly apply the results to problems and make informed decisions [15: 23-26].

The current media literacy program in the United States includes a section about the Internet. N. Willard, J. Patchin, W. Potter, E. Thoman, R. Hobbs, S. Hinduja in their articles highlight the criteria for evaluating the Internet resources to help children effectively analyze, comprehend and critically perceive information on the Internet. For example, to develop skills for critical evaluating an online resource, children should answer the following questions, including evaluating content, sources, data and site structure.

To evaluate the quality of the site, children should answer the following questions:

Criteria for Evaluating the Quality of a Web Site

Evaluation the content of the site	– Who is this resource for? What is its purpose? What information does it contain? – What is the full scope and accuracy of information on the site? To do this, you should refer to comments, other sources, if possible, not electronic. – What is the full scope and accuracy of information on the site? To do this, you should refer to comments, other sources, if possible, not electronic. – What other print or electronic sources are available on this topic? – Determine the value of the considered source in comparison with other source on this topic? – Determine the date of site creation and the date of documents creation? – How full is the topic of the site's information? – What are the criteria for selecting links to other online resources on this site? – Does the information of the referenced resources allow to create a holistic impression on the subject under study? – What additional information is contained in the Internet resources (links) on this site? – How accessible is the information on this site? – What is the value of this site's information? Is there access to multimedia resources? – Is there access to multimedia resources?
Evaluation of sources and data	– Who is the author of this site? (An individual, government organization, firm, etc.) – What purpose was it created for? (to explain, inform, convince anything). – Do the authors use methods of persuasion, propaganda? – How accurate are the facts presented on the site (do they have bibliography, references to authoritative sources, research)? – How reputable is its developer or developer team? – How fully do they have information about this issue? – Who sponsors this site (if any)? – Could the sponsors this reflect the content of the site? – When was the site designed and published? – When was its last update? – How fresh and reliable are the links? – Are any links broken? – Is there contact information for contacting the site developer?
Site structure evaluation	– What does a graphic design of a site look like? – Do the content icons match? – Do the authors adhere to the rules of spelling and speech culture writing text? – Is there a creative element in the creation of the site? – How often is this site visited? – Does the site have direct links to search engines? – Is the site overloaded with various multimedia resources?

According to the scholars mentioned above, with the help of these questions, children are able to evaluate the quality of information and select only reliable Internet resources. Such tasks will not only form the skills for working on the Internet, but also provide information protection of the child [7: 56-78; 12: 243-401].

M. Kaiser in her articles emphasizes that in most American schools children master information security through warnings and bans. Numerous instructions include a list of content that should be blocked in educational institutions [13: 78-80].

Based on publications by such scholars as S. Bazalgette, D. Buckingham, B. Duncan, R. Kubey, W. Potter, K. Tyner, C. Felitzen we can conclude that the main tasks of lessons for the formation of information protection of children on the Internet are:

1) Children should possess critical thinking, accurate evaluation and selection of information on the Internet;
2) Children should have knowledge about the risks and dangers of the Internet environment that could be harmful to health, as well as the negative consequences of disseminating negative or prohibited information;
3) Children should know about the means of spreading negative information on the Internet;
4) Teachers should familiarize children with international principles and norms and American legal regulations governing information protection of children on the Internet;
5) Teach children the rules of responsible and safe use of Internet network services;
6) Teach children how to protect themselves against dangerous activities on the Internet (cyberbullying, sexting, bulicide, etc.);
7) prevention of Internet addiction and game addiction;
8) prevention of children's offenses on the Internet [7: 45-214; 8: 150-183].

An array of American scientific publications has helped identify the basic knowledge and skills that children need for safe work online:

– Children should have critical thinking skills, be aware of the online dangers and know what categories of sites they need to avoid.

– Children should not download and install unknown software on their work and home computers.

– Children should not correspond with strangers or make appointments with virtual acquaintances without the permission of parents. A virtual interlocutor can impersonate him/herself by another person. If meeting is necessary, a child should make an appointment in a public place and tell parents about the meeting.

– Children should not open suspicious emails, files or web pages sent by strangers.

– Registering on different Internet resources use only a nickname, do not tell anyone your passwords from personal pages on the Internet network.

– Never give confidential information to anyone (name, phone number, address, school number, passwords) without parental permission. You should get parental or teacher permission to post personal photos and videos, post them on servers that restrict access to third parties.

– Follow rules and prevent plagiarism when using material posted on the Internet in the public domain.

– Remember that information which put on the Internet remains there for a long time or forever, so after the session it is recommended to delete everything related to the personal space of the user.

– Behave politely on the Internet, do nothing that may offend others or run counter to the law.

– If something is unclear, disturbs or threats you on the Internet (in an email,

on a website, in a forum, in a chat), you should always seek the help of your parents or teachers.

– Always check information from the Internet through additional requests and referrals to proven sources.

– Ask your parents for advice before making an online purchase or paying for any service.

– Always abide by the online family safety rules [7: 45-115; 8: 103-146; 12: 385-401].

According to most American scholars, following these rules will provide children with appropriate information security when working with Internet resources.

Conclusions and research perspectives. Thus, the Internet in the modern world is a powerful information and entertainment resource for children, but at the same time, child safety in the virtual space is one of the most urgent problems in the development of pedagogy and education, in particular in the USA. Information protection of children from the risks and dangers of the American Internet network is provided by legal regulations and legislative acts, software for blocking and filtering unacceptable content and websites, parental controls, efforts by teachers and school administrations to create a positive school climate, providing of the Internet network course in media education at schools where children have the skills to think critically, search and carefully select information, formation of information literacy through which children gain knowledge and ability to work properly and safely on the Internet, through the activities of health and community organizations, through extracurricular programs and activities for children and parents, by scientists and publicists. Therefore, it can be concluded that the pages of American pedagogical press highlight the opportunities, strategies, methods, approaches and sufficient experience of applying them in practice in the field of information protection of children.

Prospective directions for further development of this problem are: a detailed study of each of the methods, principles, approaches and means of information protection of children on the Internet in the USA, because experience in this field, in our opinion, will facilitate a more effective process of development of media literacy in Ukraine.

REFERENCES

1. *Children's Internet Protection Act (CIPA).* Retrieved from https://www.fcc.gov/consumers/guides/childrens-internet-protection-act [in English].

2. *Children's Online Privacy Protection Rule (COPPA).* Retrieved from https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule [in English].

3. Considine D., Haley G. (1999). *Visual Messages.* Englewood, Colorado: Teachers Ideas Press, 34 [in English].

4. Feilitzen, C., von, Carlsson, U. (2002). *Children, Young People and Media Globalisation.* Goteborg: NORDICOM, Goteborg University, 67-154 [in English].

5. Frechette, J. (2005). Cyber-Democracy or Cyber-Hegemony? *Exploring the Political and Economic Structures of the Internet as an Alternative. Library Trends, vol. 53, № 4,* 555-575 [in English].

6. Hobbs, R. (2007). *Reading the media: media literacy in high school English.* NY: Teachers College, Columbia University, 190 [in English].

7. Hobbs, R. (2011). *Digital and media literacy: connecting culture and classroom.* Thousand Oaks, CA: Corwin Press, 214 [in English].

8. Johnson, D. (2001). Computer Ethics. *Upper Saddle River.* NJ: Prentice Hall, 103-187 [in English].

9. Kubey, R. (1997). Media Education: Portraits of an Evolving Field. *Media Literacy in the Information Age.* New Brunswick, London: Transaction Publishers, 2-9 [in English].

10. Livingstone S., Haddon L. (2009). Introduction: kids online: opportunities and risks for children. In: Livingstone, Sonia and Haddon, Leslie, (eds.). *Kids online: opportunities and risks for children.* The Policy Press, Bristol, UK, 1-6. [in English].

11. Milosevic, T. (2015). Cyberbullying in US Mainstream Media. *Journal of Children and Media, vol. 9, issue 4,* 492-509 [in English].

12. Potter, W. (2011). *Media literacy.* Los Angeles: Sage, 243-401 [in English].

13. Tyner, K. (1998). *Literacy in the Digital World: Teaching and Learning in the Age of Information.* Mahwan, NJ: Lawrence Erlbaum Associates, 78-80 [in English].

14. Vaala, S., Bleakley, A. (2015). Special Issue: Children and Media in the Family Context. *Monitoring, Mediating, and Modeling: Parental Influence on Adolescent Computer and Internet Use in the United States, vol. 9, issue 1,* 40-57 [in English].

15. Worsnop C. (1999). *Screening Images: Ideas for Media Education.* Mississauga, Ontario: Wright Communications, 23-26 [in English].

Received: August 08, 2019
Accepted: September 04, 2019