dr Julia Nowicka, mgr Marta Zaroślak
War Studies University

ACTIVITIES FOR PROTECTION OF YOUNG CYBERSPACE USERS

SUMMARY

The study indicates actions taken to ensure the safety of minor network users. Prophylactic activity and methods of reacting in the case of identification of perpetrators of prohibited acts are described. It was assumed that in the area of cybersecurity, avoiding threats concerns the educational space, hence information, education and social campaigns play an important role in contemporary social functioning. The study presents the formal and legal framework for the protection of cyberspace users, the functioning of which is determined, among others, by the Convention on the Rights of the Child, the Penal Code, the International Convention on Cybercrime, the Act on Counteracting Drug Addiction, Internet Management Forum, Safer Internet Centers, Scientific and Academic Computer Network. (NASK), Empowering Children Foundation and others. Examples of assumptions of selected social programs building a safe environment for the exchange of information on the Internet are presented.

Keywords:
threats, Internet, security, cyberspace

INTRODUCTION

The modern reality of people's functioning, especially those at young age, is related to navigating in cyberspace. Based on the interpretation of the Civil Code, the age limit for minors is 18 years of age, assuming no marriage obligations . Taking into account recorded today low age of initiation in the field of contacts with the Internet (the child's seventh year of life), a young citizen is exposed to numerous dangers on the Internet, especially considering that adolescence is a time of shaping attitudes, building mutual relations as part of the need to feel the social community and the emerging social and communicative competences of individuals. If we adopt the definition that

social competences are acquired skills that condition the effectiveness of human functioning in various social situations , it is easy to notice that social exposure and the ability to assertively behave are among the factors that enable the conscious selection of content and relationships encountered in the web.

A number of threats and their manifestations concern areas related to hate speech, hate, solicitation of prohibited acts, drug addiction or broadly understood sexuality, an area particularly important for adolescent citizens, which is related to the psychophysical determinants of entering adulthood and confirming one's gender identity. It is worth noting that the need for security and development is the basic social and personal need of every human being , but it is of particular importance among young people, whose personal formation process is in the phase of strong development.

Polish law prohibits the dissemination and public presentation of so-called hard pornography, i.e. materials presenting deviant content, containing violence and brutality, as well as the use of an animal. Despite formal prohibitions, for many years children have been an object of sexual interest in cyberspace. According to the report of the Safer Internet program in Poland, minors grooming online in 2007 was reported to helpdesks 116 times . By 2010, that number had risen to 450 . In 2017, the Dyżurnet.pl team noticed many reports of profiles on social networks, which, according to the reporters, were owned by people with paedophile tendencies . In 2018, 16% of incidents reported to the Polish police concerned online child seduction .

Despite the fact that the phenomenon of psycho manipulation has not been penalized so far, the law distinguishes situations that result from this type of manipulation or result from the risks associated with it. Despite the illusion, Internet-based creativity is not an area of impunity, and authors of harmful content can be held legally liable. Applicable legal provisions may apply to creators of dangerous content, such as criminal liability for crimes, civil liability for infringement of personal rights or for committing a prohibited act or order liability for violating the regulations of a given website.

Undoubtedly, the preventive importance in the area of cybersecurity concerns educational elements, hence information, educational and social campaigns play an important role in the contemporary social functioning.

LEGAL PROTECTION OF MINORS IN CYBERSPACE

The document, which is a fundamental international legal act concerning the protection of children from harm caused to them, is called the Convention on the Rights of the Child. It was adopted by the General Assembly of the United Nations on November 20, 1989, and ratified by the President of the Republic of Poland under the Act of September 21, 1990 on the ratification of the Convention on the Rights of the Child. The content regulated by the Convention on the Rights of the Child includes, inter alia, the following articles :

- Article 8 regulating measures to enforce the child's rights to preserve their identity - nationality, surname or lawful family relationships - and to provide adequate assistance and protection in the event of violations;
- Article 16, which deals with the violation of the child's privacy - prohibits unlawful interference with private, family and home life, as well as arbitrary interference with correspondence and attacks on the honour and reputation of the child;
- Article 19 relating to all forms of violence, whether physical or psychological, harm, neglect, mistreatment and exploitation, including the sexual exploitation of children;
- Article 34 dealing with issues related to the sexual exploitation of children and sexual abuse of young people - it concerns mainly actions that should be taken to prevent:

- inducement or coercing a child into any illegal sexual activity;
- the exploitation of children for prostitution or other illegal sexual practices;
- child abuse in pornographic performances and materials.

As the Convention created in the 1980s did not yet take into account the characteristic specificity of cyberspace, the issues of child pornography were clarified by creating an Optional Protocol to the Convention on the Rights of the Child . It regulates the problem of child pornography on the Internet and orders the penalisation of its production, distribution, circulation and possession.

The International Convention on Cybercrime was adopted by the Council of Europe in November 2001 and regulates issues related to the problem of sexual abuse of children on the Internet. The Convention is a consequence of the provisions of the Convention on the Rights of the Child and speaks of measures to be taken in law for such offenses as :

• producing child pornography for the purpose of its dissemination by means of a computer system;

• offering or making available child pornography by means of a computer system;

• disseminating or transmitting child pornography via a computer system;

• procuring child pornography through a computer system for oneself or for another person;

• Possession of child pornography on a computer system or on a computer data storage medium.

All the above-mentioned international documents recommend setting the age limit for protecting children from harm at the age of 18 years. Internal, national legal regulations concerning the issue of child abuse are often the result of the ratification of international documents. Regulations at the level of Polish law include several legal acts that regulate various areas of possible threats. In the Penal Code, we can find several important provisions that regulate the safety of children and young people in cyberspace. In the case of many of them, the prosecution of the offender takes place at the request of the victim - in this case, they must file a bill of indictment with the criminal department of the appropriate District Court. Selected content of the articles is presented below. Offenses against freedom:

• Article 190, concerning criminal threats, ie raising a person's fear that a crime will be committed to the detriment of him or her or a loved one ;

• article 190a., Concerning persistent harassment or stalking and impersonating another person, aimed at creating a feeling of danger, causing material or personal harm ;

• Article 191, which deals with the use of unlawful threats or violence to compel an individual to act, refrain from or abolish him ;

• article 191a, which concerns the use of violence, unlawful threats or deception in order to record the image of a naked person or a person during sexual activity and disseminating this image without the consent of the documented person .

Offenses against sexual freedom and decency:

• Article 200, which deals with the prohibition of sexual intercourse and the inducement of a person under the age of 15 to submit to or perform sexual activity; it also prohibits the dissemination of pornographic content to children under the age of 15, and the advertising and promotion of this type of content

in a way that allows minors to reach them; in addition, the article talks about penalties for the presentation of sexual activity for sexual gratification ;

• article 200a., Concerning grooming, i.e. establishing contact with a child under the age of 15 via an ICT system or telecommunications network for the purpose of sexual activities or producing or preserving pornographic content - perpetrators may be punished for trying to meet a minor by deliberately introducing the child in error, exploiting the error, taking advantage of the inability to properly understand the situation or through threats ;

• article 200b, which prohibits the promotion and praise of paedophile behaviour ;

• article 202, deals with imposing perception of pornographic content on persons who do not wish to do so; the article also talks about imprisonment in connection with the recording, importing, storing, possessing and disseminating pornographic materials with the participation of a minor (also with his created or processed image), with the presentation of violence or the use of an animal .

Offenses against honour and bodily inviolability:

• article 212, concerning defamation of another person with conduct or properties that may consequently degrade him in the public opinion or expose him to loss of trust required in the position held ;

• article 216, also dealing with a form of insult, but in the presence or absence of a humiliated person, but with the deliberate intention that the insult reaches the person blamed .

Offenses against public order:

• article 256, talking about the penal consequences for promoting a fascist or other totalitarian system of the state, it also prohibits incitement to hatred on the basis of national, ethnic, racial and religious differences - the penalty is foreseen for producing, recording, importing, acquiring, storing, possessing, presenting, transporting or sending materials containing content that promotes a totalitarian regime or encourages hatred (artistic, educational, collector and scientific creators are exempt from punishment) ;

• Article 257., which prohibits publicly insulting and violating the physical integrity of persons or groups based on their national, ethnic, racial or religious affiliation .

Offenses against information protection:

• article 267, dealing with unlawful access to information by hacking into a network, bypassing its security, or using eavesdropping and visual devices ;

• Article 268a, which deals with any destruction, damage, deletion, alteration or obstruction of access to data; it also talks about disrupting or preventing the processing, collection or transfer of IT data.

It is worth noting that articles 256 and 257 do not protect people who are insulted because of their age, disability, political and professional affiliation or sexual orientation .

PROTECTION OF MINORS IN TERMS OF SELECTED THREATS

Documents such as the Act on Counteracting Drug Addiction contain additional provisions that facilitate the fight against online threats. Article 20 of the Act concerns the prohibition of advertising and promotion of psychotropic substances , narcotic drugs, substitutes or psychoactive substances, and Article 58 prohibits giving, facilitating and enabling the use or inducing a person (including minors) to use narcotic drugs, psychotropic or psychoactive substances .

The effects of actions taken to counteract computer crime against minors are :

• international legislative projects;

• cross-border law enforcement cooperation;

• international educational projects;

• exchange of practices aimed at improvement of activities.

In 1996, with the adoption of the Plan to Combat Racism and Xenophobia, the subject of online safety was addressed by the European Union. A year later, in 1997, the Telecommunications Council adopted a Resolution on harmful or illegal content on the Internet and the declaration Illegal and harmful content on the Internet was issued by the European Commission. Shortly thereafter, the Action Plan for promoting safe use of the Internet by combating harmful or illegal content on global networks, developed by the Parliament and the European Council, prompted the launch of the Safer Internet Action Plan - SIAP by the European Commission.

Outside the European Union, the safety of children and adolescents online is a topic taken up in the United States Organization - in November 2007, the problem of protecting minors online was discussed within the Internet

Governance Forum, convened by the UN Secretary General. The convening of the Forum took place on July 18, 2006 as a platform for discussion and exchange of information about policies and practices related to technology, including the Internet. IGF is an advisory body - its meetings are open and allow for understanding and exchange of knowledge on how to get the most out of the Internet, and how to deal with the risks and challenges that come with its use . In Poland, Forum meetings have been organized since 2016, and the conclusions and recommendations of the meetings are presented at world conferences. Topics dealing with the problems of the digital economy based on data, artificial intelligence, innovative technologies, digital competences and finally security, enable a global discussion about the development of the Internet. It is worth mentioning that the next World Internet Governance Forum will be organized by the Ministry of Digital Affairs in November 2020 in Katowice. It will be attended by government representatives, entrepreneurs, scientists and NGOs from around the world .

In Athens, in 2006, at the Internet Governance Forum, the concept of dynamic coalitions, i.e. open groups dealing, among others, with issues of Internet governance, was created. The Dynamic Coalition on Child Online Safety (DCCOS) can be found among the many groups formed. The idea behind this coalition was to ensure the safe use of the opportunities offered by the Internet and modern technologies, and to address the risks associated with their use at the global, regional and national levels.

The coalition requires stakeholders to engage in activities such as :

- protection against potentially harmful content, behaviours and contacts;
- disrupting the production and distribution of child sexual abuse images and videos;
- disrupting all forms of sexual exploitation, including exploitation through the misuse of modern technology.

INHOPE is a network of 47 national awareness centres, located around the world, working together through a network of Safer Internet Centres (SICs) in Europe. They include information centres, helplines, hotlines and youth panels . Their mission is to support hotlines in the fight against online child sexual abuse . Helplines provide information, advice and support to children and adults via telephone, internet forms or messengers. Topics covered include dealing with harmful content, harmful contacts, and harmful behaviours (such

as cyberbullying and sexting) . Hotlines allow users to anonymously report illegal content available on the web. These reports are consequently forwarded to the relevant authorities, such as the police or the relevant INHOPE hotline . Youth panels allow young people to exchange views, knowledge and experience on the use of new technologies and tips related to online safety .

The goal of the trusted response teams network is to eliminate CSAM content and to support the creation of national procedures to remove illegal content from the web as quickly as possible . INHOPE is supported, among others, by Interpol, Europol, INSAFE and global companies from the IT sector, and its activities are co-financed by the European Commission.

PROTECTION OF MINORS IN TERMS OF SELECTED THREAT

The Connecting Europe Facility (CEF) program supports European networks and infrastructure in the transport, telecommunications and energy sectors. The European Commission has proposed a series of guidelines for the purpose and priorities of digital services and broadband networks . CEF supports digital service projects that aim to improve the quality of life of society through access to technology, connectivity, interoperability and the development of the digital market. Examples of sectors supported by the program include cybersecurity, e-signature, e-invoicing, e-delivery, e-identification and automatic translation . In Poland, the Connecting Europe Facility strategy is implemented by NASK and the Empowering Children Foundation.

The Scientific and Academic Computer Network (NASK) is a research and development unit that develops solutions to increase the efficiency, reliability and security of ICT networks and network systems. It was established in 1991 as the Coordination Team of the Scientific and Academic Computer Network at the University of Warsaw, and as an independent unit it has been operating on the Polish market since 1993 . From the very beginning, the main goal of NASK was to provide access to the Internet for scientific and academic institutions, as well as to conduct research on the use of new technologies and on network security. Currently, the main stream of the Institute's research is broadly understood cybersecurity, including reacting to events that violate security on the network and coordinating activities in this area. For this purpose, the structure of the institute includes the CERT Polska (Computer Emergency Response Team) and the Dyżurnet.pl team, which deal

with the registration, handling and classification of events that violate Internet security . In accordance with the act on the national security system, the NASK Institute was appointed as one of the Computer Security Incident Response Team (CSIRT), which serves to coordinate incidents reported by key service operators, digital service providers, local government and the users themselves.

Since 2005, NASK, together with the Empowering Children Foundation, have been implementing the Safer Internet program of the European Commission and running the Dyżurnet.pl project that accepts reports of illegal content online. The Scientific and Academic Computer Network is a state institute cooperating with the Ministry of Digitization and the Central Information Technology Centre, which implements social projects and training for companies and institutions concerning, above all, security issues. In 2017, the institute became the operator of the National Education Network (NEN) program, which aims to connect Polish schools to fast and safe Internet.

The Empowering Children Foundation (formerly Nobody's Children Foundation) is a non-governmental organization operating since 1991, which aims to ensure a safe childhood for children and to treat them with respect for their dignity and subjectivity. The Foundation deals with the protection of children from harm, as well as helping them minors who have experienced violence. It conducts research and provides assistance in the discussed area.

The main mission of the FDDS is :

- psychological and legal assistance for abused children and their guardians;
- children's education - how to prevent violence and abuse;
- adult education - how to treat children and help them prevent being harmed;
- adult education - what to do in case of suspected child abuse;
- influencing the law to effectively protect children.

The Foundation educates children, parents and professionals in the field of counteracting violence against minors, developing the ability to respond to threats, strengthening educational competences and effective methods of intervening in cases of potential child abuse. It also runs an educational platform where one can find educational materials, lesson plans and e-learning courses. In addition to the materials available under the Safer Internet program, the Foundation provides scenarios of activities that can help children,

adolescents and their caregivers to learn to function on the Internet and to cope with its risks. Among the many available, it is worth paying attention to Zuźka and Tunio get to know the Internet (cartoons and puzzles aimed at introducing the youngest children to the basic mechanisms of functioning in cyberspace and teaching effective and safe use of the Internet), Day of Life (intended for students of the oldest elementary classes and aimed at the problem of excessive use of the Internet), My online image (intended for conscious and responsible image creation on the web), Fejsmen's Adventures (devoted to the image and privacy in the virtual world), The Art of Search (devoted to improving the skills of methods of searching and verifying content on the Internet) and Stop Cyberbullying (intended for cyberbullying and ways of dealing with this form of peer violence). The Empowering Children Foundation also publishes guides and brochures on the use of the Internet and online safety.

The Orange Foundation was established in 2005, its activities are directed primarily to young people - from learning the basics of online safety (MegaMission project) to programming, but also to adults - the foundation created an online guide about online safety for parents, and created materials for teachers, thanks to which they can conduct classes (digital education project Lesson: Enter). The Foundation also conducts a series of studies related to the safe use of telecommunications networks and media.

Initially, in the years 1999-2014, the Safer Internet program was implemented under the European Commission program, which focused on promoting safe use of the Internet and new technologies among children and adolescents. Due to intensive technological development, in 2005 the program was extended to also include mobile networks, online games, file sharing via peer-to-peer networks and all forms of real-time communication on the network (such as chats and instant messaging). Since 2015, the project has been financed under the Connecting Europe Program, thanks to which Safe Internet Centres operate in all European Union countries. The Polish Safer Internet Program Centre (PCPSI) was established in 2005 and is made up of the state-owned research institute NASK, which is also the PCPSI coordinator, and the Empowering Children Foundation. The Orange Foundation is the partner of most of the projects implemented by PCPSI. The Polish Centre aims to promote safe use of the Internet among children and young people and more effective use of the Internet and new technologies. The Centre conducts comprehensive awareness-raising activities through educational campaigns, media campaigns,

international conferences and regular seminars. It also prepares promotional materials, expert publications and organizes the Safer Internet Day celebrations .

The main assumptions of the program include activities such as :

- combating illegal content;
- counteracting harmful content;
- promoting a safe online environment;
- raising awareness of online threats.

Under PCPSI, three largest and most important undertakings are carried out - the Safer Internet, helpline.org.pl and dyzurnet.pl projects. Safeinternet.pl is a program that aims to increase public awareness of threats. Its educational activities are aimed at children and adolescents, parents and guardians, as well as specialists - including teachers and policemen. The Safer Internet program conducts social campaigns targeting all users of the Internet. The Child on the Web deserves the most attention (the campaign is aimed mainly at parents, its aim is to sensitize them to the effects of children's contact, especially in preschool and early school age, with harmful materials on the Internet), Offline challenge (the challenge of completely cutting off from the Internet for 48 hours in order to discover their own habits related to the use of the Internet), Attentive parents (its key elements are a short film, brochures, website and articles aimed at keeping the child safe online), I think therefore I don't send (an educational program addressed to young people, their parents and people working with teenagers, the aim of which is to raise young people's awareness of the consequences of sexting), You can help - react, report! (addressed to Internet users exposed to the presentation of CSAM content), Think before you buy (its aim is to help adults make a conscious choice of electronic devices bought for children) or Mom Dad a tablet (warning against making electronic devices available to the youngest children too early) . Among the materials for the education of children and adolescents, you can find content adapted to children of all ages - from kindergarten to high school, for example: Necio.pl (addressed to children aged 4 to 6, whose aim is to learn how to use the Internet safely), File and Folder (a project for children between 6 and 13 years old, talking about threats such as Internet and computer abuse, cyberbullying, as well as talking about positive ways of using the Internet to develop and present their passions) and Sieciaki.pl (a website for somewhat older children - 9-11 years old, which aims to provide a comprehensive dose of knowledge in the field of Internet safety and prevention of online threats) . An integral part of the Sieciaki.pl website is the BeSt browser, which allows you to view websites only from the BeSt safe website directory. The catalogue contains websites and portals assessed by specialists and classified in age and

thematic categories . Among the materials for increasing knowledge in adults, you can find the project Become your child's friend, aimed at encouraging parents and guardians to actively participate in the Internet life of their pupils, and to check whether children's activity does not threaten their proper development . Safer Internet also runs a project aimed at young people - Digital Youth, which concerns online safety and the valuable use of new technologies and consists of a blog (digitalyouth.pl), a Facebook profile, a paper magazine, an annual forum and meetings with young people. Most importantly, the organizations participating in the Safer Internet program also organize Safer Internet Day celebrations involving countries from all over the world.

SUMMARY

Among the most important documents and legal acts regulating dangerous phenomena, including psycho-manipulation of minors in cyberspace, are the Convention on the Rights of the Child, the International Convention on Cybercrime, the Penal Code, the Act on Counteracting Drug Addiction and others. For the effective operation of response teams, cooperation at both national and international levels is essential. Cooperation must be established with Internet users, with Internet service providers as well as with law enforcement authorities.

National Awareness Centres focus on raising awareness and understanding of online safety issues by running campaigns to raise both children and adults knowledge, skills and strategies to ensure online safety and take advantage of the opportunities offered by new technologies. Public and private sector institutions and non-profit organizations play a significant role in building online safety among minors. Their social, educational and charitable activities spread knowledge about how to use new technologies wisely and responsibly. The more actions and community activities in the field of security while using the Internet, the less victims of threats awaiting users in cyberspace. One of the forms of initiatives in this area is the Safer Internet Day (SID). Initiated by the Insafe network in 2004, it is an international event that takes place in February each year to promote the safe and responsible use of the Internet by children and young people. The aim of SID is to initiate and promote activities for online safety and to promote the use of opportunities offered by the use of the Internet. The idea of this day is to highlight the power

of cooperation to achieve online security, both locally and internationally . In Poland, the Safer Internet Day (SID) has been organized since 2005 by the Polish Safer Internet Centre. The patronage over this day is taken by the Ministry of Digital Affairs, the Ministry of National Education, the Commissioner for Citizens' Rights and the Police Headquarters. Every year, PCPSI undertakes activities to implement the effective celebration of the Safer Internet Day, including: organizing a conference addressed to representatives of the education sector, non-governmental organizations and people working with children, as well as organizing local initiatives for online safety, such as educational activities, happenings, campaigns information, contests.

It seems that the key to building the protection of minors in cyberspace is the systemic cooperation of state, local and private entities and all kinds of foundations, while increasing individual and group education in the field of real and potential threats functioning in cyberspace.

BIBLIOGRAFIA

[1] Bochenek M., Lange R. (eds.), *Teenagers 3.0*., Ed. NASK, Warsaw 2019.

[2] Matczak A., *Questionnaire of Social Competences, Publisher: Psychological Test Laboratory of the Polish Psychological Association*, Warsaw 2011.

[3] Ciekanowski Z., Nowicka J., *Military threats to state security* [in:]*Determinants of military security*, Wróblewski R., Wyrębek H. (ed.), Institute of Social Sciences and Security, University of Natural and Humanities in Siedlce, Siedlce 2016.

[4] Wrzesień-Gandolfo A. (ed.), *Safety of children online*, Polish Safer Internet Center, Warsaw 2014.

[5] The Convention on the Rights of the Child, adopted by the United Nations General Assembly on November 20, 1989 (Journal of Laws No. 120, item 526).

[6] Council of Europe Convention on Cybercrime, drawn up in Budapest on November 23, 2001. (Journal of Laws 2015, item 728).

[7] The Act of 23 April 1964 - Civil Code (Journal of Laws No. 16, item 93).

[8] Act of 29 July 2005 on Counteracting Drug Addiction (Journal of Laws of 2005, No. 179, item 1485).

[9] The Act of June 6, 1997, Penal Code (Journal of Laws of 1997, No. 88, item 553).

[10] Optional Protocol to the Convention on the Rights of the Child on the trafficking of children, child prostitution and child pornography, adopted in New York on May 25, 2000 (Journal of Laws No. 76, item 494).

[11] Dyżurnet.pl, Report 2017, https://dyzurnet.pl/download/multimedia/raporty/raport_2017.pdf.

[12] Dyżurnet.pl, Report 2018, https://dyzurnet.pl/download/multimedia/raporty/raport_2018.pdf.

[13] Empowering Children Foundation, Children's and Youth Contact with Pornography, https://fdds.pl/wp-content/uploads/2017/12/Makaruk_K_Wlodarczyk_J_Michalski_P_2017_Kontakt_dzieci_i_mlodziezy_z_pornografia.pdf.

[14] Empowering Children Foundation, Problematic use of the Internet by young people, https://fdds.pl/wp-content/uploads/2020/01/Problematyczne-u%C5%BCwanie-internetu-przez-m%C5%82odzie%C5% BC.-Raport-z-examines% C5% 84.pdf.

[15] Nobody's Children Foundation, Report: Safety of children using the Internet, Bezpiecznaszkola.men.gov.pl/wp-content/uploads/2015/09/raport-bezpieczenstwo-dzieci-zystajacych-z-internetu.pdf.

[16] Nobody's Children Foundation, Seksting Among Polish Youth, http://fdds.pl/wp-content/uploads/2016/05/Wojcik_Makaruk_Seksting_wsrod_polskiej_mlodziezy.pdf.

[17] Orange Foundation, Safe media, https://fundacja.orange.pl/files/user_files/user_upload/materialy_edu_dla_nauczycieli/Poradnik_Bbezpieczne_media/Bbezpieczne_media._Pwiedznik_dla_rodzicow.pdf.

[18] https://ec.europa.eu/digital-single-market/en/safer-internet-day-sid.

[19] https://ec.europa.eu/digital-single-market/node/151.

[20] https://fdds.pl.

[21] https://fdds.pl/o-przegladarce-best.

[22] https://fundacja.orange.pl/o-fundacji/o-nas.

[23] https://www.betterinternetforkids.eu/web/poland/profile.

[24] https://www.betterinternetforkids.eu/web/portal/policy/insafe-inhope.

[25] https://www.edukacja.fdds.pl.

[26] https://www.inhope.org/EN/our-story.

[27] https://www.intgovforum.org/multilingual/content/about-igf-faqs.

[28] https://www.intgovforum.org/multilingual/content/dynamic-coalition-on-child-online-safety-dccos.

[29] https://www.nask.pl/pl/o-nas/kim-jestesmy/3261,O-NASK.html.

[30] https://www.saferinternet.pl/kampanie-spoleczne.html.

[31] https://www.saferinternet.pl/o-nas/safer-internet-w-europie.html.

[32] https://www.saferinternet.pl/o-nas/safer-internet-w-polsce.html.

[33] https://www.saferinternet.pl/projekty/projekty-edukacyjne.html.

[34] Safer Internet Program in Poland, Annual Report on the implementation of Awareness, Helpline and Hotline projects, https://www.saferinternet.pl/pliki/publikacje/raport2007.pdf.

[35] Safer Internet Program in Poland, Report on the implementation of Awareness and Hotline 2005–2006 projects, https://www.saferinternet.pl/pliki/publikacje/raport_PL.pdf.

ACTIVITIES FOR PROTECTION OF YOUNG CYBERSPACE USERS

ABSTRACT

The study indicates actions taken to ensure the safety of minor network users. Prophylactic activity and methods of reacting in the case of identification of perpetrators of prohibited acts are described. It was assumed that in the area of cybersecurity, avoiding threats concerns the educational space, hence information, education and social campaigns play an important role in contemporary social functioning. The study presents the formal and legal framework for the protection of cyberspace users, the functioning of which is determined, among others, by the Convention on the Rights of the Child, the Penal Code, the International Convention on Cybercrime, the Act on Counteracting Drug Addiction, Internet Management Forum, Safer Internet Centers, Scientific and Academic Computer Network. (NASK), Empowering Children Foundation and others. Examples of assumptions of selected

social programs building a safe environment for the exchange of information on the Internet are presented.