Readiness of The Future Preschool and Primary Education Specialists to form the Foundations of Children's Cyber Security

Oleksandra Shykyrynska
Valentina Voloshyna Faculty of Preschool and Primary Education
Vinnytsia Mykhailo Kotsiubynsky State Pedagogical University, Vinnytsia, Ukraine
o.v.shikirinska@gmail.com

Valentyna Liapunova
Educational and Scientific Institute of Social-Pedagogical and Artistic Education.
Bogdan Khmelnitsky Melitopol State Pedagogical University
Melitopol, Ukraine
lapunova001@gmail.com

Olha Melnykova
Faculty of Preschool and Special Education
Pavlo Tychyna Uman State Pedagogical University
Uman, Ukraine
olga@maistruk.com

Kateryna Mnyshenko
Valentina Voloshyna Faculty of Preschool and Primary Education
Vinnytsia Mykhailo Kotsiubynsky State Pedagogical University, Vinnytsia, Ukraine
katerinamazur7@gmail.com

Tetiana Petryshyna
Valentina Voloshyna Faculty of Preschool and Primary Education
Vinnytsia Mykhailo Kotsiubynsky State Pedagogical University, Vinnytsia, Ukraine
tetanapetrisina21@gmail.comt

Abstract. **In connection with the digitization of the educational process, the need for the development of critical thinking of children of senior preschool and junior school age, the development of the ability to use information in any form, to communicate, and to be aware of the consequences of interaction in the digital world is increasing. The article found out that the training of the future preschool and primary education specialists should include the formation and development of methodological competence of students in order to develop in children of preschool and junior school age the ability to protect themselves, their information and privacy on the Internet, the ability to be friendly and brave on the Internet, formation of serious attitude to privacy and security. The experimental research has been conducted, the respondents of which were bachelor's degree students of the specialty 012 Preschool Education and 013 Primary Education of Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University. The following approaches and technologies for forming the ability of the future preschool and primary education specialists to form the basics of cyber security for preschool and primary school children have been highlighted: the problem-based approach, BYOD technology ("bring your own device"), the method of "flipped learning". The results of the approbation with bachelor's degree students of the speciality 012 Preschool Education and 013 Primary Education of the educational guide on children's security on the Internet, developed by Google in cooperation with The Net Safety Collaborative and the Internet Keep Safe Coalition and evaluated by the Scientific Center "Crimes Against Children" of the University of New Hampshire, have been given.**

Keywords: educational process of primary school, junior schoolchildren, educational process of preschool education institution, media literacy, information culture, innovative BYOD technology.

I. INTRODUCTION

Children get acquainted with digital devices at an early age. They see that parents and relatives use such devices. Imitating their parents, children start using a tablet, touch phone, and laptop from an early age. Therefore, it is necessary to start familiarizing children with possible threats on the Internet from the youngest age, to form the ability to use gadgets safely. Another

Print ISSN 1691-5402
Online ISSN 2256-070X
https://doi.org/10.17770/etr2024vol2.8087

problem is that many parents do not understand the importance of forming the foundations of children's information culture and cyber security. Parents use tablets and a phones so that the children do not disturb them at home. Another problem is that parents do not know the basics of their own information security. Various threats await the child on the Internet, such as sexual content, communication with strangers, revealing personal and parents' data.

In connection with the digitalization of the educational process (Ciarko, M., & Paluch-Dybek, A. (2021); Otterborn, A., Sundberg, B., & Schönborn, K. (2024)), the need to develop critical thinking of children of senior preschool and junior school age is increasing Choiriyah, C. (2021). It is necessary to develop the ability to use information in any form, to communicate, to be aware of the consequences of interaction in the digital world Martin, F., Gezer, T., Anderson, J., Polly, D., & Wang, W. (2021). On the one hand, digital devices create more opportunities for children's learning, and on the other hand, the use of mobile apps, touch phones and tablets for entertainment can affect their safety in the digital world (Chassiakos et al., 2016). Another threat is intimidation on the Internet, social media, cyberbullying and other threats and addictions (Li, 2006). The use of mobile devices and tablets by children under the age of 7 without adult supervision is a problem, because children do not have critical thinking, do not know how to make independent decisions and cannot predict their own actions (Sziron & Hildt, 2018).

We found a contradiction between the speed of development of digital technologies and fraudulent activities on the Internet and the training of preschool and primary education specialists.

II. Materials and Methods

In the course of this research, we used the following methods: theoretical: analysis of scientific sources to determine the state of research on the formation of the readiness of the future preschool and primary education specialists for children's cyber security, synthesis, systematization and generalization of the theoretical provisions of the problem; empirical: pedagogical observation of the activities of children in preschool education institutions, conversations with students about knowledge of the basics of cyber security, conversations with educators of preschool education institutions regarding the conduct of classes or games on children's cyber security, questionnaires of the future preschool and primary education specialists of Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University.

III. Results and Discussion

The research was conducted in the period from September to December 2023. 73 full-time bachelor's degree students and 22 part-time bachelor's degree students of the 3rd year of study of the Faculty of Preschool and Primary Education named after Valentyna Voloshyna, specialty 012 Preschool Education of Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University (Vinnytsia, Ukraine) took part in the survey.

The online survey was distributed through personal connections of the researchers. The researchers shared the results of the online survey on social media and email. The survey window was open for 6 months from September 2023 to January 2024. Participation in the online survey was voluntary.

The objective of this survey was to find out the current level of readiness of the future preschool and primary education specialists for the formation of the basics of cyber security of children of preschool and primary school age. For this, appropriate criteria have been developed and their indicators determined: motivational (need for professional and personal growth; desire for new knowledge in the field of cyber security); cognitive (knowledge about threats and addictions on the Internet); activity (the ability to distinguish between threats and addictions on the Internet and to form the foundations of children's cyber security).

Three levels of readiness of the future preschool and primary education specialists to implement the basics of children's security have also been characterized.

High – expressed motivation for continuous self-development and improvement in the field of children's cyber security with readiness to implement advanced pedagogical approaches; deep knowledge and understanding of threats and dependencies on the Internet; the ability to apply practical experience in the basics of cyber security in professional activities.

Sufficient – growing awareness of the importance of professional and personal development in the field of children's cyber security, active self-assessment and identification of gaps for self-improvement; understanding of the range of methods and technologies of manipulations, threats, dependencies on the Internet; the ability to apply knowledge about children's cyber security on the Internet in practical situations;

Low – insufficient understanding of the importance of professional and personal development in the field of children's cyber security; basic knowledge of the theoretical foundations of the formation of children's cyber security; limited readiness to use knowledge in practical activities.

The respondents were offered a survey in Google Forms, which included three blocks of questions, according to selected criteria.

We used the following two questions to find out the levels of readiness of the future preschool and primary education specialists for the formation of the basics of children's cyber security based on the motivational criterion. The first was the following question: "How important is it for an educator to engage in self-education in the field of digital security?" Justify your opinion. Give at least three reasons for justification. If the student mentioned three or more good reasons, then this is a high level, if only one – it is sufficient, if he or she did not mention any or this reason was insignificant, then it is low. According to the results of the answer to this question, the level of 18 students is high, 45 students have sufficient, and 32 – low level of readiness.

In order to find out whether the future specialists use the given arguments in their own lives, we proposed the

second question: "What courses have you taken in the last six months on information culture?" If the respondent named at least two courses, it was a high level, if one – sufficient, if none – low. Thus, 15 students have a high level, 37 have a sufficient level, and 43 have a low level. Based on the results of two questions, we can determine the levels of readiness of the future preschool and primary education specialists according to the motivational criterion: high 17, sufficient 41, low – 37.

The next block of questions was aimed at identifying the levels of readiness of the future preschool and primary education specialists for the formation of the basics of children's cyber security according to the cognitive criterion. The first question was: "Which of the submitted can be fake: fact, news, computer, antivirus, video, photo, piece of information, theorem, site, account, program?" If the student chose more than three correct answers it was a high level, at least three – a sufficient level, one or none – a low level. The results are as follows: high – 27, sufficient – 39, low – 29.

The future preschool and primary education specialist should be well aware of all the threats and addictions that await an unprepared user on the network. The next question was to find out such knowledge. We offered a list of threats and addictions: happy slapping, "dancing pigs", "fb shower", "phubbing", scams, voyeurism, greed for information, selfies, tablet zombies. The respondent had to place them in two categories: category one – threats, category two – addictions. If the student made one mistake during placing, this is a high level, if two to four it is sufficient, more than four – low. Results: high – 20 students, sufficient – 32 students, low – 43. The generalized data according to the cognitive criterion are as follows: high – 24, sufficient – 36, low – 35.

In order to familiarize children with the basics of cyber security, the future preschool and primary education specialist must have the ability to verify information himself or herself. The next block of questions is aimed at identifying the levels of readiness of the future specialists for the formation of the basics of cyber security of children of preschool and younger school age according to operational criteria. The first question was: "How to check if the information is fake?" Students indicated that they need to check all events, names, processes listed in the information on at least three different sites. The results should be the same. If we cannot find the name of a famous person mentioned in the information or we notice other discrepancies, most likely, this information is fake, that is, untrue. In order to check this, students were asked to check whether such information is true. Information. Once every five years, the awarding ceremony of one of the world's main art prizes is held. This is happening in the homeland of outstanding painters: Michelangelo, Caravaggio and Raphael – in Italy. All these five years, their respected descendants carefully follow the talents of the brush from all over the planet, in order to discover the most gifted and skilled. Therefore, it is especially pleasant that this time the experts chose an artist – a young and talented, and from now on, an artist recognized by the world – Mykola Bezkorovainyi. "We are all extremely impressed by the simplicity and at the same time the power of the artistic expressions of this young artist", said the curator of the prize, Gert Jan Jansen. "I have not seen anyone more gifted and at the same time wise and modest. So I am sure: we should be proud of such an artist". Students who indicated all three signs that the information is fake – high level, only one – sufficient, those who said that the information is true – low level. Results: high level – 16 students, sufficient – 56, low – 36.

The next question is: "How important do you think it is to talk about building the basics of children's cyber security with parents of preschool children? Justify your opinion". If the student gave three or more arguments, this is a high level, if one – it is sufficient, if there were no arguments, it is low. Results: high – 35 students, sufficient – 44 students, low – 16. As we can see, in the answer to this question there are the most students of high and sufficient levels. In our opinion, this is caused by the specifics of the pedagogical institution in which the future preschool and primary education specialists receive their education. Generalized data on the readiness of the future preschool and primary education specialists to form the basics of children's cyber security according to operational criteria: high – 26, sufficient – 50, low –19. Generalized data according to three criteria can be seen in Table 1.

TABLE 1.LEVELS OF READINESS OF THE FUTURE PRESCHOOL AND PRIMARY EDUCATION SPECIALISTS FOR THE FORMATION OF THE BASICS OF CHILDREN'S CYBER SECURITY

	High	Sufficient	Low	Total
motivational	17	41	37	95
cognitive	24	36	35	95
operational	26	50	19	95

We also observed the educational process in 14 preschool education institutions in the city of Vinnytsia. The results of the observation are as follows: in 10 kindergartens, educators do not conduct activities on children's cyber security. The reason was found out in personal conversations with educators. Since children are not allowed to use gadgets in kindergarten, they consider cyber security work to be the parents' business. In four other kindergartens, educators conduct special discussions, games, and quests with the aim of children's cyber security.

To increase the level of knowledge of the future preschool and primary education specialists in the basics of children's cyber security, we offer students selective disciplines "Media education and formation of information culture of preschool and primary school children", "Formation of the basics of cyber security of preschool and primary school children". In the course of teaching these disciplines, we emphasize the interaction of the educator of the preschool education institution with parents regarding the formation of the basics of cyber security for children of preschool and primary school age.

We also used the educational guide on children's security on the Internet during two academic years, namely: 2021-2022 and 2022-2023. The guide was developed by Google in cooperation with The Net Safety

Collaborative and Internet Keep Safe Coalition. In cooperation with the non-profit organization Committee for Children, the authors created new social-emotional educational activities that will help children in their travels through the digital world. The guide on children's security on the Internet has been evaluated by the University of New Hampshire's Crimes Against Children Research Centre. Based on the results of the research conducted by the centre, this is the first guide on children's security on the Internet that has been proven to have a positive impact on teaching children about online security and digital citizenship. The guide on children's security on the Internet is a self-contained resource. All practical tasks can be completed without special professional skills, with minimal training and without special equipment or other learning resources. In addition, the material learned at the lessons can be put into practice in a fun and interesting way thanks to the online adventure game Interland. The guide covers five fundamental topics on digital citizenship and security: share wisely (digital footprint and responsible communication); don't be fooled (phishing, scams and trusted sources); keep your secrets (online security and passwords); it's cool to be friendly! (combating negative behaviour on the Internet); do you doubt? Ask! (doubtful content and scripts).

This guide is designed for grades 2-6, but the lessons will be useful for teachers of both older and younger children, including sections on terms, class discussions and games. We encourage you to experiment and choose the program that works best for your pupils. For example, you can go through the entire program from start to finish, or you can focus on a few lessons that your pupils need most. In addition, you can use resources for teachers and parents: ready-made slides, printables, a manual and tips for families to use at home. International Society for Technology in Education (ISTE) conducted an independent audit of the guide on children's security on the Internet and recognized it as a resource that helps prepare pupils for the ISTE 2021 Standards and awarded with the Seal of Alignment for Readiness.

While working with this guide, we used the following approaches and technologies of the formation of the future preschool and primary education specialists in the ability to form the basics of cyber security of children of preschool and junior school age: problem-based approach, BYOD technology ("bring your own device"), the method of "flipped learning". At the beginning of each practical lesson, before explaining a new topic, we asked students problematic questions. For example, during the study of the topic "I don't mean it" (module 1, lesson 3), students were asked whether they encountered the phenomenon of non-understanding or misunderstanding of certain information by others. Such a problematic question prompted students to be motivated in perceiving a new topic. Since students and teachers of Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University work remotely during martial law, they used BYOD technology ("bring your own device") during practical classes, giving students the task of finding certain information using their own devices. The method of "flipped learning" was also used. For this, on the eve of the practical lesson, information was posted for familiarization in the virtual environment of Google Classroom. This material was discussed directly with the students in the form of a conversation during the practical lesson. We also noticed that this approach contributes to a stronger memorization of the material.

ACKNOWLEDGMENTS

We express our gratitude to the teachers and students of the Department of Pre-school Education of the Mykhailo Kotsiubynskyi Vinnytsia State Pedagogical University, to the teachers of Pre-school Education Institution No. 30 and 27 in the city of Vinnytsia

CONCLUSIONS

In the article, the authors made an attempt to actualize the problem of readiness of the future preschool and primary education specialists to form the foundations of children's cyber security. In connection with the increase of threats on the Internet and the use of gadgets by children from an early age, it is necessary to develop children's ability to use the Internet safely, to be conscious citizens of the digital world. In this regard, it is necessary to train the future preschool and primary education specialists.

The following approaches and technologies for forming the ability of the future preschool and primary education specialists to form the foundations of cyber security of preschool and primary school children have been highlighted: problem-based approach, BYOD technology ("bring your own device"), the method of "flipped learning".

The conducted research does not cover all aspects of the problem under consideration. The question of forming the motivation of preschool and primary education specialists for independent continuous professional development in the field of cyber security requires further research.

REFERENCES

[1] A. Ciarko, and A.Paluch-Dybek, (2021). The importance of digitalization in the education process. In *E3S Web of Conferences* (Vol. 307, p. 06002). EDP Sciences.

[2] AOtterborn, B. Sundberg, and K. Schönborn, (2024). The impact of digital and analog approaches on a multidimensional preschool science education. *Research in science education*, *54*(2), 185-203.

[3] C. Choiriyah, (2021). Science literacy in early childhood: Development of learning programs in the classroom. *Indonesian Journal of Early Childhood Education Studies*, *10*(2), 136-142.

[4] Y. L. R. Chassiakos, J. Radesky, D. Christakis, M.A. Moreno, and C. Cross, (2016). Children and adolescents and digital media. Pediatrics, 138(5), e20162593. https://doi.org/10.1542/peds.2016-2593

[5] F.Martin, T. Gezer, J. Anderson, D. Polly, and W. Wang, (2021). Examining parents perception on elementary school children digital safety. *Educational Media International*, *58*(1), 60-77.

[6] Q. Li, (2006). Cyberbullying in schools: A research of gender differences. School Psychology International, 27(2), 157–170. https://doi.org/10.1177/0143034306064547