BULGARIAN ACADEMY OF SCIENCES
PROBLEMS OF ENGINEERING CYBERNETICS AND ROBOTICS • 2026 • Vol. **84**, pp. 21-34
p-ISSN: 2738-7356; e-ISSN: 2738-7364
https://doi.org/10.7546/PECR.84.26.02

Assessment of Teachers' Preparedness in Cybersecurity

Radoslav Yoshinov[1], *Neda Chehlarova*[2], *Galina Dishkova*[3]

[1] *Laboratory of telematics at Institute of mathematics and informatics – Bulgarian Academy of Sciences,*
[2] *Institute of robotics "St. Ap. and Gospeller Matthew" – Bulgarian Academy of Sciences,*
[3] *Institute of mathematics and informatics – Bulgarian Academy of Sciences*
Emails: yoshinov@cc.bas.bg, nedachehlarova@ir.bas.bg, g.dishkova@math.bas.bg

Abstract: Data from an anonymous survey conducted in 2024, with secondary school teachers from Bulgaria, who received a one-time short cybersecurity training is presented. The study includes a self-assessment of cybersecurity knowledge and skills – devices used, cyberattack prevention options, protection tools, authentication, and more. Recommendations are made regarding further activities to support teachers in using protective methods and follow-up actions in the event of a cyberattack/cyberbullying, as well as to increase their competence in helping students.

Keywords: Cybersecurity, Cyberbullying, Digital competence, Self-assessment, Teachers, Education.

1. Introduction

There is a growing need for cybersecurity knowledge when working or communicating in an online environment. The reason is the increased share of the use of the Internet by society, both personally and professionally, with different purposes, as well as with the development of the types of attacks and, accordingly, the means of protection [1], [2], [3], [4], [5], [6], [7], [8].

Within the framework of the educational process in the country, conditions have been created for communication at a distance; access to digital resources and scripts; virtual environments for self-training; recommendations for using artificial intelligence in education; STEM spaces in schools with internet access capabilities; short television shows with a focus on the development of citizens' digital competence and others [9], [10], [11], [12], [13], [14], [15], [16], [17], [18].

In-class training, as well as extra-curricular training, presupposes teachers' competence in cybersecurity. Therefore, it is important to periodically evaluate this cybersecurity competency. In this regard, the current article presents the results of a survey conducted anonymously during the period from 29.04. until 27.05.2024. through Google Forms.

In "Hristo Botev" Secondary School, Septemvri city, in October 2023, a two-hour training was held with pedagogical specialists on the topic "Cyberbullying and the role of the school in combating it" with emphasis on: the genesis of the problem and the definition of cyberbullying children; where is the cyberspace around me; the role of pedagogical specialists in solving problems; effective problem solving model; main directions in the problem; using a secure network (Wi-fi) and the dangers it entails; passwords; practical solutions and methodology developed by the Agency for Child Protection in Cyberspace – Israel; social networks.

2. Problem description

In connection with planning further activities to support teachers at "Hristo Botev" Secondary School in Septemvri city, it is necessary to conduct an anonymous survey to gather information on their current readiness to use protective measures and to follow up on actions in the event of a cyberattack/cyberbullying.

3. Methodology of conducted survey

For the purposes of conducting an anonymous survey on teachers' readiness to use protective measures and to follow up on actions in the event of a cyberattack/cyberbullying, a survey consisting of 18 questions was developed and presented at the end of the article. THIS survey was implemented using Google Forms, and the results obtained are analyzed in the next section.

4. Analysis of results

In the study participated 36 teachers from SU "Hristo Botev" in Septemvri city. Students from the 1st to the 12th grade are trained in it. In Fig. 1 is shown the age distribution of the participants. The largest number of representatives are from 51 to 60 years of age – 33%. Teachers under the age of 30 are 19%. The next age group has a similar value – 17% are between 30 and 40 years old. The distribution by gender is expected for the profession in the country – 81% indicated female and 17% male.

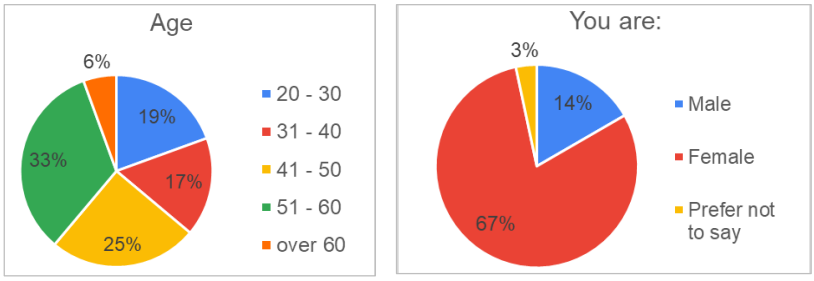

Fig. 1. Age and gender distribution of surveyed teachers.

All respondents have a higher education, with 78% having a master's degree (Fig. 2).

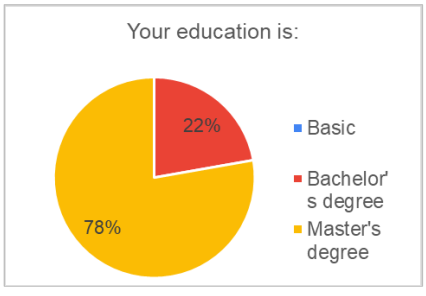

Fig. 2. Last completed education of the surveyed teachers.

According to the data from Fig. 3 a total of 31% are primary teachers, which equals 1/3 of the teaching staff.

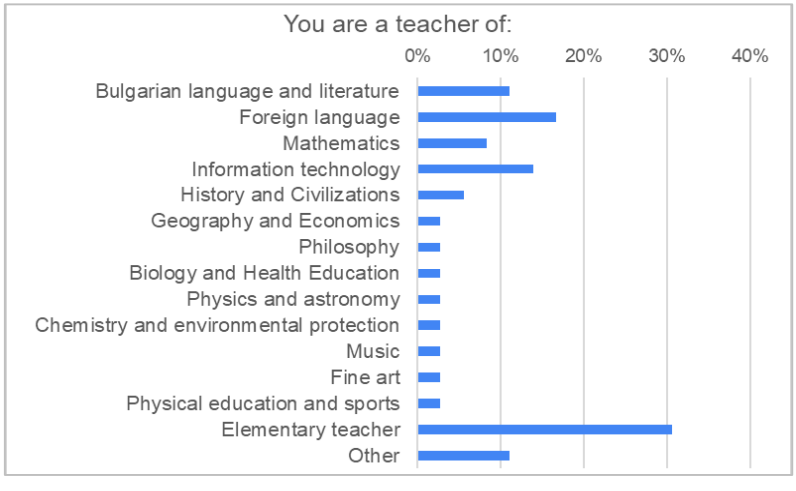

Fig. 3. Teaching area of the pedagogical staff.

In the team there are several specialists in Foreign Language, Information Technology, Bulgarian Language and Literature, Mathematics. A total of 5 teachers indicated that they teach the subject Information Technology. Of them, three also lead classes in a second subject – two in Mathematics and one in Physics and Astronomy.

In Fig. 4 is presented the data on the number of teachers working with students from the 1st to the 12th grades, inclusive. Nearly 30% of the school's teachers work with students from V to VII.

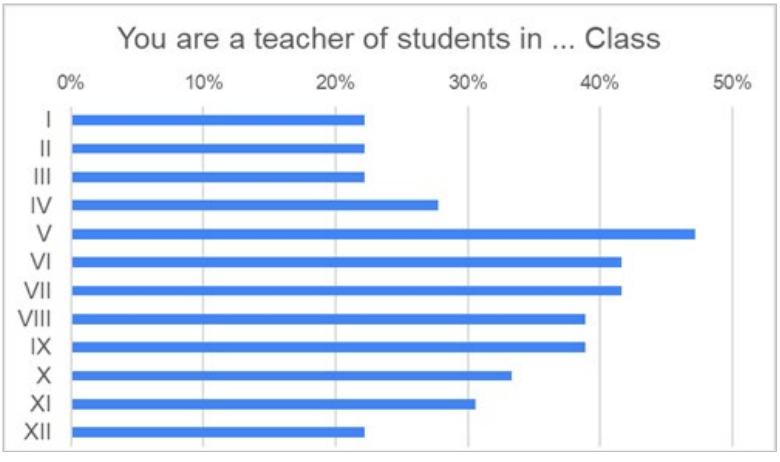

Fig. 4. You are a teacher of students in … grade.

Two teachers specified that they work with all classes – the school psychologist and the pedagogical advisor. The next ones working with the most students are:

- History and Civilization teacher – in V, VI, VII, VIII, IX, X, XI, XII grades;
- Teacher of Mathematics, Information Technologies – in V, VI, VII, VIII, IX, X, XI, XII grades;
- Music teacher – in I, III, IV, V, VI, VII, VIII, IX, X grades.

There is a variety of teachers according to the years of teaching experience. The data from Fig. 5 are comparable to those concerning the age of teachers (See Fig. 1) and confirm them.

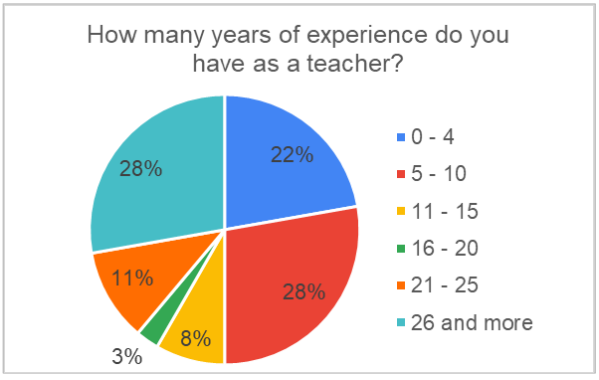

Fig. 5. Experience as a teacher.

According to the data from Fig. 6. mobile phone and laptop are used by 94% of teachers to access the Internet. The desktop computer has twice as little usability – 39%. The remaining 2 devices are indicated below 10% – a tablet and a smart watch/bracelet.

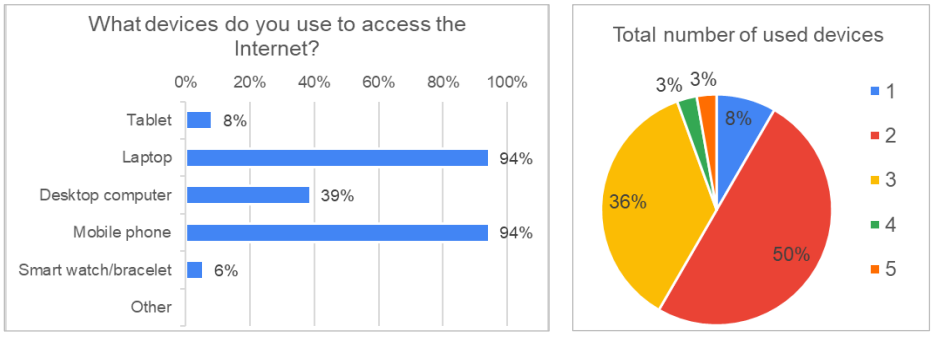

Fig. 6. Devices used to access Internet.

All teachers indicated at least 1 device through which they access the Internet. Only 1 respondent noted that they use all 5 device types. He specified that he is a teacher of the subjects Information Technology and Physics and Astronomy. The majority of teachers (50%) work with up to 2 devices – a tablet and a mobile phone. Another 36% work with the same two devices and a desktop computer, or a total of 3 means of accessing the Internet. The duration of Internet use per day is varied (Fig. 7).

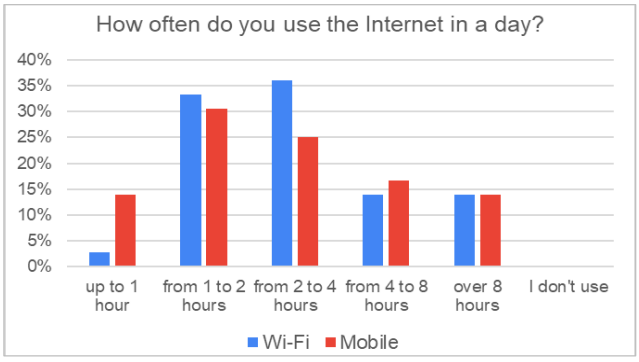

Fig. 7. Amount of Internet usage time per day.

All respondents use the Internet. The periods "from 1 to 2 hours" and "from 2 to 4 hours" have the highest values - from 25% to 36%, both when using Mobile Internet and when using Wi-Fi. "Over 8 hours" of using both types of Internet were noted by two respondents – a teacher of Chemistry and Environmental Protection, a teacher of Mathematics. Both teachers are with Master degree with teaching experience of "5-10" years and teach in classes from V grade upwards.

Over 39% of the respondents know all the listed 7 threats related to information security. "Viruses, worms and Trojan horses" is the most familiar threat among teachers with 89% indicating. However, all threats are to some extent unknown to respondents. A total of 28% of respondents know all 7 threats. Of 5 teachers teaching the subject of Information Technology: 1 knows all threats, 1 does not know them, and the remaining 3 are partially aware (Fig. 8).

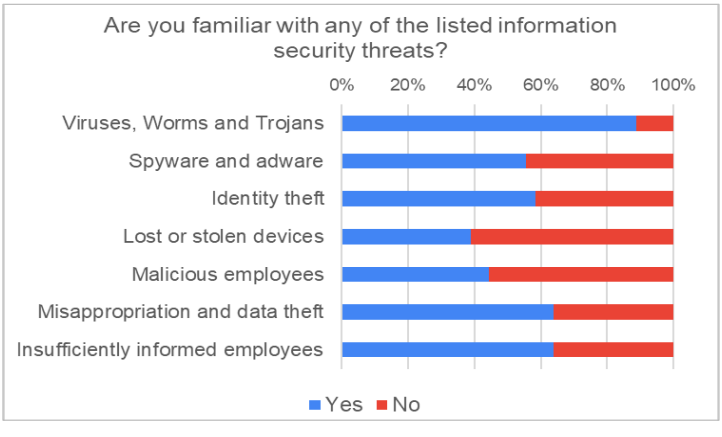

Fig. 8. Knowledge of information security threats.

Of the mentioned means of protection, only the "Antivirus program" is known to all respondents and 89% of them use it. Over 36% of teachers do not know the other 5 protective measures. The least used are "Disk encryption", "VPN", "Written information security policy" (Fig. 9).

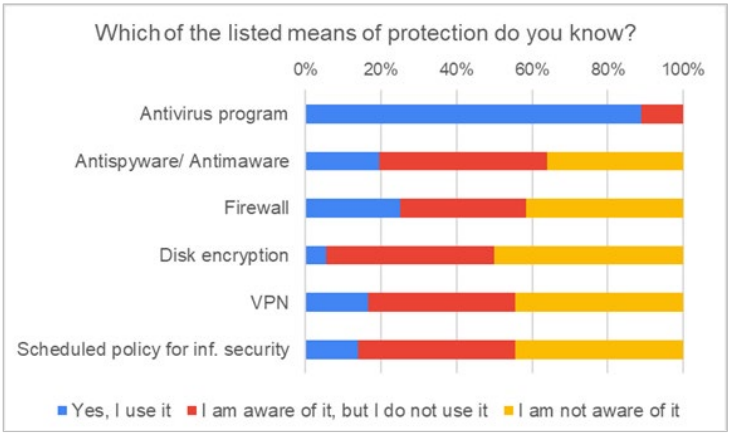

Fig. 9. Degree of awareness of means of protection.

Although the teachers went through a short training a few months ago, all the mentioned options for multi-factor authentication are to some extent unknown to the respondents (Fig. 10). The most unfamiliar to teachers, with more than 50% indicating, are "Authy" and "Vein Recognition", which is not used by any respondent. The most frequently used authentication methods are fingerprint (42%) and SMS (50%).

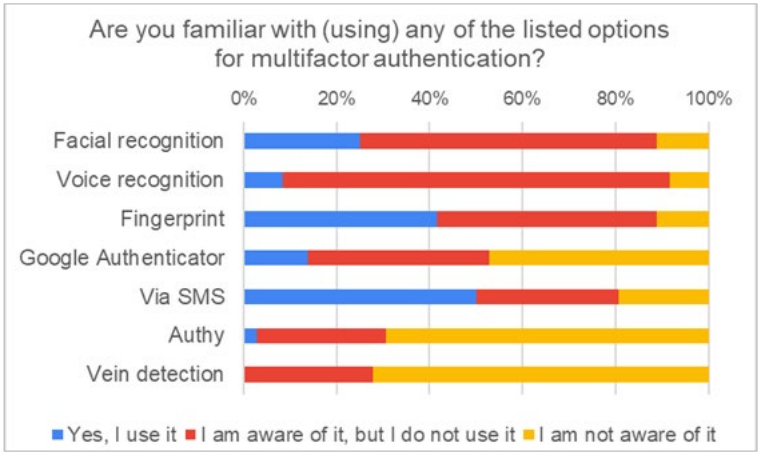

Fig.10. Awareness of multi-factor authentication options.

Of the respondents, 22% believe that they have been a victim of a cyberincident/cybercrime, but do not provide specific information about the case (Fig. 11).

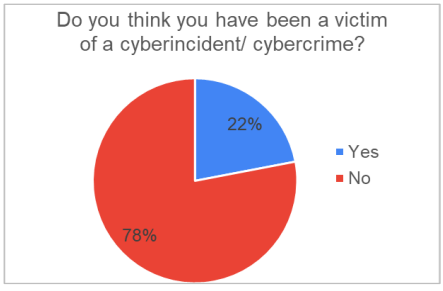

Fig.11. Self-assessment of experienced cyberincident or cybercrime.

All teachers have undergone at least 1 training in the last 5 years, on a topic developing their digital competence. Most teachers participated in training related to "digital resources" – 67%. Trainings on "digital communication technologies" and "cyber security" were attended by 47% and 50% of respondents, respectively. Of the five "Information Technology" teachers, two have been trained in "cyber security". There is no teacher trained in "artificial intelligence" and "robotics". Only 3 teachers have gone through the training on all 3 subjects marked at all. The remaining teachers participated in one (47%) or two (44%) trainings in this regard, during the same period (Fig. 12).

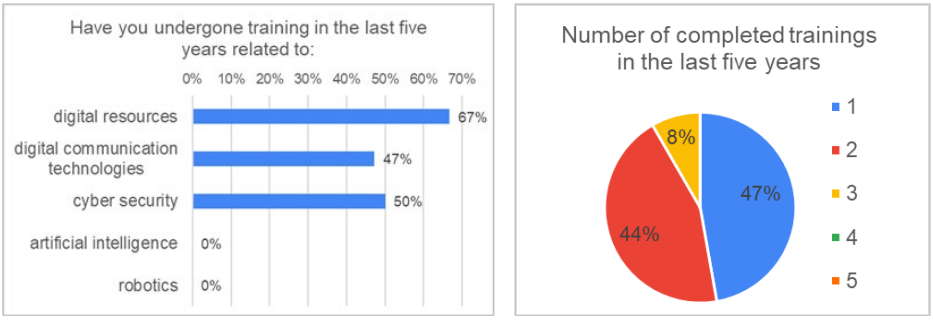

Fig.12. Training received by teachers in the last five years related to their digital competence.

33.3% of the teachers were approached by students, sharing about a case of cyberbullying (Fig. 13).

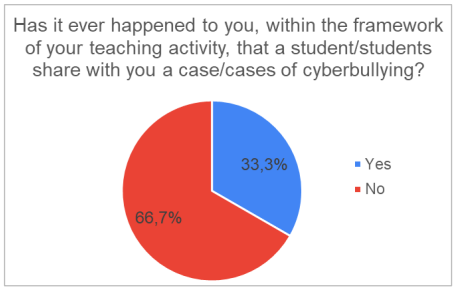

Fig.13. Student sharing rate of cyberbullying.

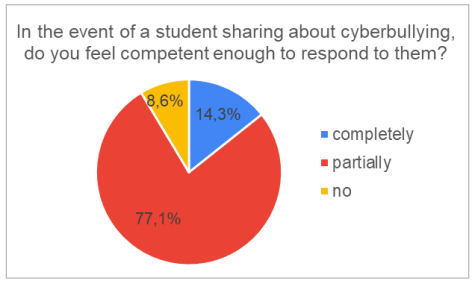

Fig.14. Self-rated willingness to support a student in sharing about cyberbullying.

14.3% of the teachers feel fully prepared to respond to a case of cyberbullying shared by a student. 77.1% of the respondents feel partially competent, and three teachers self-identified as incompetent (Fig. 14). We note that the respondents have undergone theoretical training and specified that they need practical activities to support the information received.

One of the three who indicated the answer "no" noted that knows all the threats related to information security (See Fig. 8); uses "Anti-Virus Program" and "Scheduled Information Security Policy" but does not know the other means of protection (See Fig. 9). The same teacher does not know five of the multi-factor authentication options, and knows the other two (Fingerprint, Voice recognition) but does Not use (See Fig. 10).

Desire to participate in training was indicated by 77.1% of the teachers, from 2 to 4 hours, on the topic of "Child cyberbullying" (Fig. 15), which confirms the expressed desire to develop their knowledge and skills in this area.

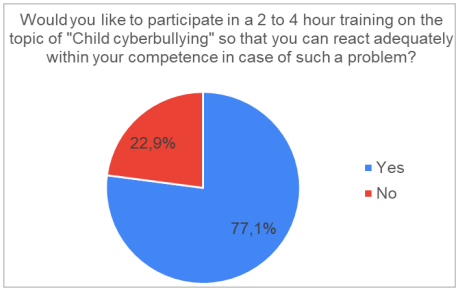

Fig.15. Willingness to participate in a 2 to 4-hour training session on "Child cyberbullying".

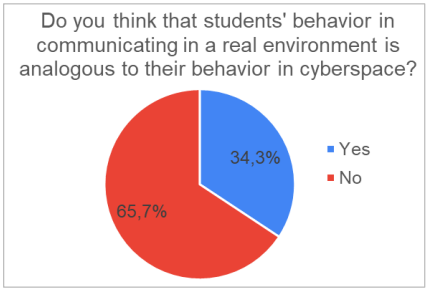

Fig.16. Assessment of the relationship between students' behaviour in a real environment and in cyberspace.

All three self-identified as incompetent to assist in case of cyberbullying (See Fig. 14) indicated that they did not want to participate in such a course and increase their competence. Two of them have experience of "5-10" years as a teacher, and the third of 26 and more years; one of the same three teachers had previously participated in “cyber security” training (See Fig. 5).

Of the teachers, who participated in previous trainings on "cyber security" (See Fig. 12), a total of 72% indicated that they would also participate in the one with topic "Child cyberbullying". Accordingly, 28% do not wish to participate in a next course on a similar topic.

The majority of teachers have observed a difference in the behaviour of students in a real environment and in cyberspace (Fig. 16).

Teachers' self-assessment of their digital competence is high (Fig. 17). Part of this self-assessment is probably due to the formed skills for creating and working with digital resources, for remote work in an electronic environment. Both their organized training and work during and after the COVID 19 pandemic have contributed to this.

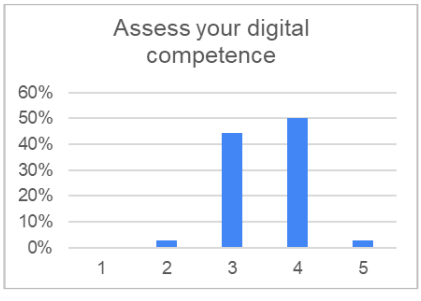

Fig.17. Self-assessment of digital competence.

After the training, all teachers expressed their satisfaction with the training and made the following recommendations:

- to hold further trainings, in which specific examples will be considered;
- to conduct training with parents;
- to conduct trainings for the majority of students.

The organization and implementation of future training/qualification courses should be supported by periodic reviews of the current level of knowledge and skills of teachers in relation to cybersecurity. The results of such surveys help in the development of cybersecurity policies, as well as the implementation of procedures for actions by pedagogical specialists in schools.

5. Conclusion

The present research shows that the teachers at SU "Hristo Botev", in Septemvri city, Bulgaria, have a responsible and conscious attitude to the problem of cyber security and cyberbullying for children, and the need for several short-term trainings on topics that are not well known to teachers is outlined, namely: types of threats related to information security; means of protection; use of multi-factor authentication; providing support to students who have been bullied online.

It is recommended that the trainings be practically oriented and include commentary on various real situations on the topics, as well as discussions with the teachers. Meetings with experts in the field of cyber security, experts from the State Agency for Child Protection, UNICEF, psychologists and/or pedagogical advisors with experience in educational institutions and others are necessary to achieve the goals of the prevention of child bullying in the online space. Organizing and holding a forum on the topic will unite the efforts of institutions at the local level in the fight against cyberbullying for children.

Acknowledgments. This work was supported by the NSP DS program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

References

1. Chehlarova, N., Tsochev, G., Kotseva, M., Miltchev, R.: Digital competencies of public administration employees related to cybersecurity. In: 2021 12th National Conference with International Participation. Electronica. IEEE. pp. 1-4. (2021)
2. Trifonov, R., Manolov, S., Tsochev, G., Pavlova, G.: Recommendations concerning the selection of artificial intelligence methods for increasing of cyber-security. In: Proceedings of the 21st International Conference on Computer Systems and Technologies. pp. 51-55. (2020)
3. Tsochev, G., Trifonov, R., Nakov, O., Manolov, S., Pavlova, G.: Cyber security: Threats and challenges. In: 2020 International Conference Automatics and Informatics. ICAI. IEEE. pp. 1-6. (2020)
4. Pirta-Dreimane, R., Brilingaite, A., Roponena, E., Parish, K., Grabis, J., Lugo, R., Bonders, M.: CyberEscape Approach to Advancing Hard and Soft Skills in Cybersecurity Education. Lecture Notes in Computer Science, 441-459 (2023).
5. Tsochev, G., Yoshinov, R.: Research on Cyber-Physical Systems Security. 1st ed. Education and Knowledge. Sofia, Bulgaria, (2020)
6. Trifonov, R., Nakov, O., Manolov, S., Tsochev, G., Pavlova, G.: Possibilities for Improving the Quality of Cyber Security Education through Application of Artificial Intelligence Methods. In: International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, pp. 1-4 (2020)

7. Steen, T.: Measuring Behavioural Cybersecurity: An Overview of Options. Lecture Notes in Computer Science, 460-471 (2023).
8. Yoshinov, R., Kotseva, M., Madzharov, A., Chehlarova, N.: Implying cybersecurity skills for public administration employees. In: Environment. Technologies. Resources. Proceedings of the International Scientific and Practical Conference. Vol. 4, pp. 300-304 (2024)
9. Gaidarski I., Minchev Z.: Insider Threats to IT Security of Critical Infrastructures. Digital Transformation, Cyber Security and Resilience of Modern Societies. Studies in Big Data, Springer, Cham, vol. 84, pp. 381-394 (2021)
10. Mashatan, A., Turetken, O.: Changing Hearts and Minds: The Role of Cybersecurity Champion Programs in Cybersecurity Culture. Lecture Notes in Computer Science, 416-428 (2023)
11. Mladenova, M.: Impact of information and communication technologies on workplaces. Part 1: Developing the concept of digital competence. European frameworks related to digital competence. Intel Entrans. Sofia. (2019)
12. Chehlarova, T.: Survey results on the degree of satisfaction and fatigue while preparing for and when conducting distance learning - March 16-20, 2020. Pedagogical Forum, 2, 39-47 (2020)
13. Chehlarova, T., Tsvyatkov, D., Chehlarova, N.: Distance Learning in "Ivan Vazov" Secondary School in Stara Zagora during the 2020/2021 school year. Strategies for Policy in Science and Education. 29(6), 568-580 (2021)
14. Minchev, Z.: On the growing transformational role of AI technologies for the future cyber diplomacy in the postinformation age. International Journal of Cyber Diplomacy. MES, 29-41. (2023)
15. National program "Building a school STEM environment" https://www.mon.bg/mon/natsionalen-plan-za-vazstanovyavane-i-ustoychivost/ 2024/09/03
16. Yoshinov, R., Chehlarova, T., Kotseva, M.: The e-facilitator as a key player for interactive dissemination of STEAM resources for e-learning via webinar. In: Auer, M.E., Tsiatsos, T. (eds.) IMCL 2019. AISC, vol. 1192, pp. 675–686. Springer, Cham, (2021)
17. MES. Guidelines for the use of artificial intelligence in the educational system. Project as of January 2024. https://www.mon.bg/nfs/2024/02/nasoki-izpolzvane-ii_190224.pdf 2024/09/03
18. Bulgarian National Television. Press F1. https://bnt.bg/bg/a/natisni-f1 2024/09/03

Appendix 1: Survey

(1) You are:
Male; Female; I prefer not to specify

(2) Age:
20–30; 31–40; 51–60; over 60

(3) Your education is:
Basic; Bachelor's degree; Master's degree

(4) You are a teacher of:
Bulgarian language and literature; Foreign language; Mathematics; Information technology; History and Civilizations; Geography and Economics; Philosophy; Biology and Health Education; Physics and Astronomy; Chemistry and environmental protection; Music; Fine art; Physical education and sports; Elementary teacher; Other

(5) You are a teacher of students in .... class:
I; II; III; IV; V; VI; VII; VIII; IX; X; XI; XII

(6) How many years of experience do you have as a teacher?:
0-4; 5-10; 11-15; 16-20; 21-25; 26 and more

(7) What devices do you use to access the Internet?:
Tablet; Laptop; Desktop computer; Mobile phone; Smart watch/bracelet; Other

(8) How often do you use Wi-Fi and Mobile Internet in a day?:
up to 1 hour; from 1 to 2 hours; from 2 to 4 hours; from 4 to 8 hours; over 8 hours; I don't use

(9) Do you know any of the listed information security threats (Yes/No)?:
Viruses, worms and Trojans; Spyware and adware; Identity Theft; Lost or stolen devices; Malicious employees; Misappropriation and data theft; Insufficiently informed employees

(10) Which of the listed means of protection do you know (Yes, I use it; I am aware of it, but I do Not use it; I am Not aware of it)?:
Antivirus program; Antispyware/ Antimalware; Firewall; Disk encryption; VPN; Scheduled policy for inf. Security

(11) Are you familiar with (using) any of the listed options for multifactor authentication know (Yes, I use it; I am aware of it, but I do Not use it; I am Not aware of it)?:
Facial recognition; Voice recognition; Fingerprint; Google Authenticator; Via SMS; Authy; Vein detection

(12) Do you think you have been a victim of a cyberincident/ cybercrime? – free answer

(13) Have you undergone training in the last five years related to:
digital resources; digital communication technologies; cyber security; artificial intelligence; robotics

(14) Has it ever happened to you, within the framework of your teaching activity, that a student/students shared with you a case/cases of cyberbullying?:
Yes/No

(15) In the event of a student sharing about cyberbullying, do you feel competent enough to respond to them?:
completely; partially; no

(16) Would you like to participate in a 2 to 4 hour training on the topic of "Child cyberbullying" so that you can react adequately within your competence in case of such a problem?:
Yes/ No

(17) Do you think that students' behavior in communicating in a real environment is analogous to their behavior in cyberspace?:
Yes/ No

(18) Rate your digital competence:
from 1 (low) to 5 (high)