*Environment. Technology. Resources. Rezekne, Latvia*
*Proceedings of the 15th International Scientific and Practical Conference. Volume IV, 300-304*

# *Implying cybersecurity skills for public administration employees*

**Radoslav Yoshinov**
*Laboratory of telematics*
*Bulgarian Academy of Sciences*
Sofia, Bulgaria
yoshinov@cc.bas.bg

**Monka Kotseva**
*Laboratory of telematics*
*Bulgarian Academy of Sciences*
Sofia, Bulgaria
mkotseva@cc.bas.bg

**Anastas Madzharov**
*Institute of Robotics "St. Ap. and Gospeller Matthew"*
*Bulgarian Academy of Sciences*
Sofia, Bulgaria
a.madzharov@ir.bas.bg

**Neda Chehlarova**
*Institute of Robotics "St. Ap. and Gospeller Matthew"*
*Bulgarian Academy of Sciences*
Sofia, Bulgaria
nedachehlarova@ir.bas.bg

***Abstract.*** **The results of a conducted study on the knowledge and skills of representatives of the public and local administration regarding cyber security in modern digital work processes are presented. The survey was conducted in 2023 in the Republic of Bulgaria. The analysis includes a comparison of the data with those of a similar survey of employees in the public administration in 2020.**

***Keywords: cybersecurity, cyberethics, digital competence, public administration, employees***

## I. Introduction

The use of ICT tools as a fundamental support of traditional processes related to management and administration has led to the term e-governance (e-government). This term does not have a clear definition, but we will accept "the use of information and communication technologies (ICT), especially the Internet, as a tool to achieve better governance". Data is now an integral part of every sector and function of government – as important as physical assets and human resources, and its management requires special attention and expert action [1]. In order to improve the digital competencies of employees in government structures, it is essential to have a prepared and well-informed administration [2] - [5]. This requires drawing a clear picture of the current state and creating a plan for progress that meets societal needs [6] - [10].

Here are analyzed the preparation and awareness of employees of the public administration, comparing the results with a similar study conducted in 2020 [11]. A part of the questions was reserved in order to report whether there is development on basic topics, such as security, problem solving, communication between individual units and citizens. The questions from 2020 have been adapted and the data in the comparative analysis is based on the number of respondents. Another part was supplemented by taking into account the new realities of progress in digital transformation and the possibilities of using artificial intelligence for the modernization and overall improvement of the functioning of public administration.

## II. Materials and Methods

The study involved two groups of public administration employees, with the first study conducted during the COVID-19 pandemic in 2020 and then repeated in 2023. Both surveys were anonymous and voluntary, and therefore different numbers of respondents participated in the different periods, with the number of participants in the first survey being over 175, and in the second over 75.

## III. Results And Discussion

The age profile of the two groups of respondents is similar and includes mostly respondents between 30 and 65 years old “Fig 1”.

*Print ISSN 1691-5402*
*Online ISSN 2256-070X*
*https://doi.org/10.17770/etr2024vol4.8238*

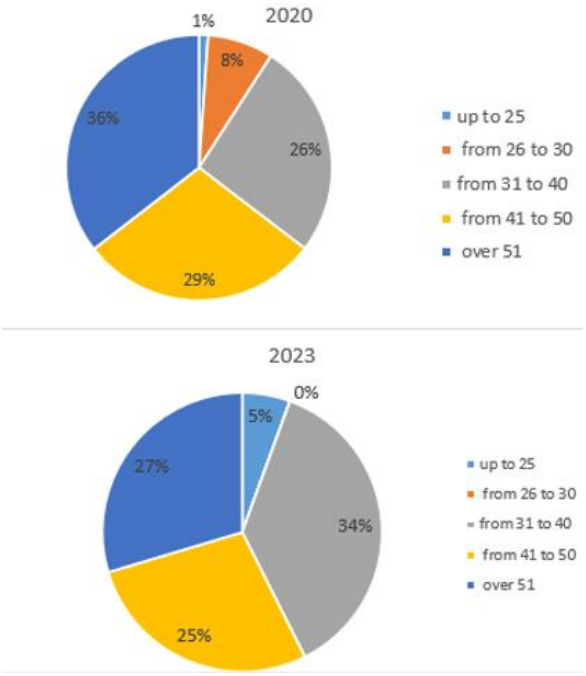


Fig. 1 Age distribution of participants in 2020 and 2023.

The distribution by gender is similar, and in the second survey it is noticed that more men took part “Fig. 2”, but again the ratio is 2:1, although according to official statistics the distribution of employees in the administration is even [2].

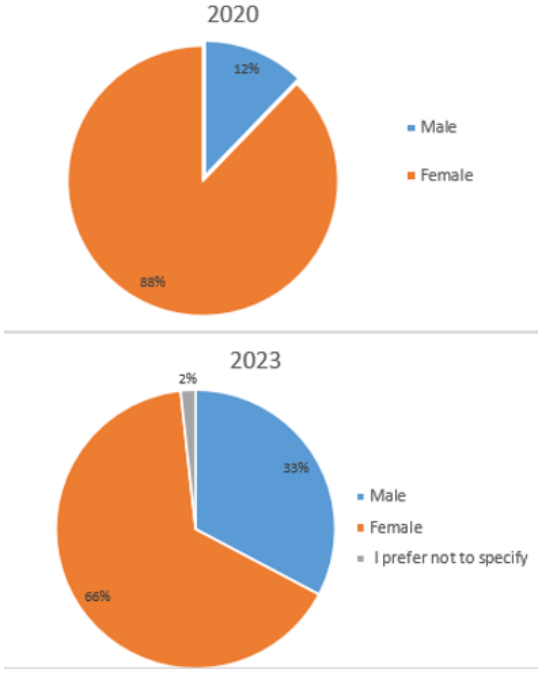


Fig. 2 Gender distribution of participants in 2020 and 2023.

During the crisis related to the spread of COVID-19, a number of activities and administrative services of the central and local authorities were put to the test. We all know that the pandemic caught us off guard and forced public authorities and many businesses to digitize their services, making them easily accessible online [12]. Data from the first survey show that although the Internet was the place for communication, those who answered the question "How much time do you use the Internet for work?" are 62% of the respondents, and the activities they perform are between 1 and 2 hours. To the question: "After and during the COVID-19 pandemic, did you have to carry out your activity electronically (without direct contact with consumers)?", 69% of the administration answered that they carried out their activity entirely on the Internet, as on 31 % of them had to perform their duties online for the first time. In proportion to the entry of technological innovations into our daily duties, new security problems also arise. By its nature, the concept of information security is of strategic importance for the interests of the individual, society and the state as a whole. In order to be able to achieve higher levels of security in the field of information technology, it is necessary to achieve a higher awareness, both about the threats to information security, and about the methods of combating the threats. This is especially important for people working in public administration. For this reason, the main emphasis in the survey was the questions related to the preparation of the employees in this direction when performing their duties.

It is known that the employees in the administration have access to many and different types of data. One of the most important data protection tools is multi-factor authentication (MFA) [12] - [13]. It uses at least two different components from the categories of knowledge, possession and biometrics for registration. Here are the results of the question: "Are you familiar with (using) any of the listed options for multifactor authentication?" “Fig. 3”:

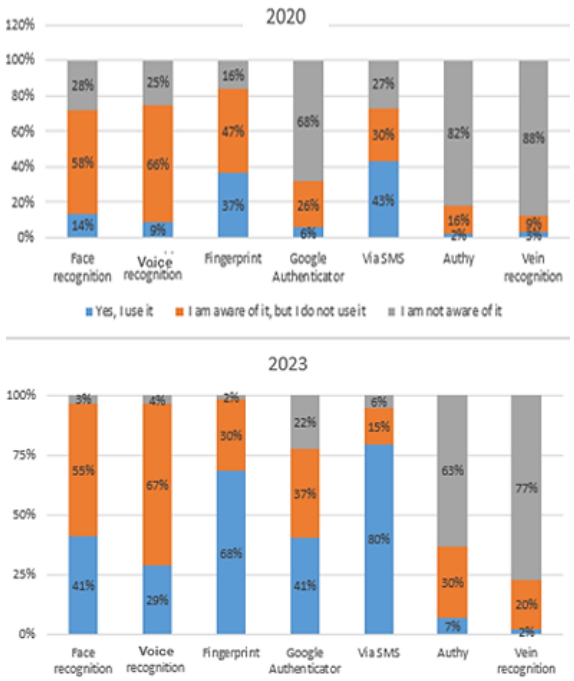


Fig. 3 Are you familiar with (using) any of the listed options for multifactor authentication.

It is noteworthy that, compared to the 2020 survey, the 2023 result shows that most of the specified authentication methods are not unfamiliar, although not all are used. The most common means of protection used are SMS and fingerprint, which have nearly doubled since 2020, with SMS being used by 80% and fingerprint by nearly 70% of respondents. Other responses that show an

increase in employee awareness and knowledge are related to the voice and facial recognition authentication group, which saw a 3-fold increase but maintained non-use rates. Two-factor authentication applications (such as Authy) and biometric vein recognition systems are still unknown and underutilized.

Information security also requires knowledge of possible threats. To the question: "Do you know any of the listed threats related to information security?" the following responses were given shown in “Fig. 4”.

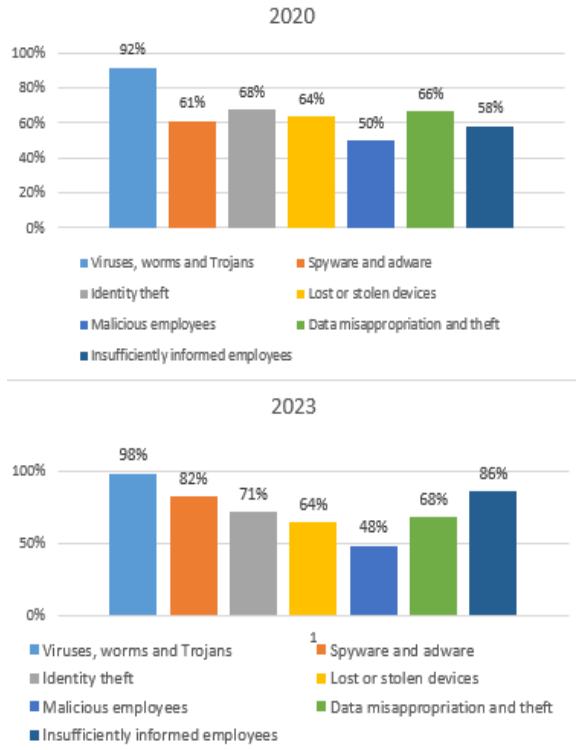


Fig. 4 Do you know any of the listed information security threats.

Viruses, worms and trojans are well known in both surveys, with 100% awareness in the 2023 survey. It is encouraging that some of the listed threats have increased awareness by between 10 - 20% [11]. Lost/stolen devices, malicious employees, and data and identity theft and misappropriation remain at the same levels, with the largest increase in the victimization rate of insufficiently informed employees, which is a natural process accompanying the greater number of services offered in the Internet space.

Another important aspect of security is the reliability of security mechanisms, knowledge and their correct use. Here is the development of responses to the question: "Are you aware of any of the information security threats listed below? “Fig. 5”.

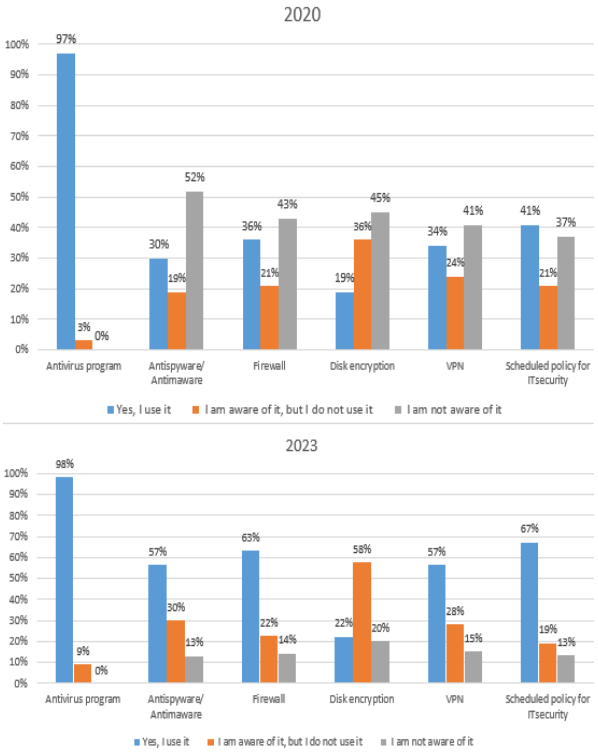


Fig. 5 Which of the following means of protection do you know.

In proportion to virus awareness, the use of anti-virus programs is close to 100%. The use of the remaining means of protection listed in the survey has grown almost twice, which speaks of an increase in the awareness of the respondents [11]. The result of knowledge of data encryption has not undergone significant change and is still not used as a way of prevention. This fact may be due to the fact that most cloud service providers use encryption, but the problem remains when it comes to data on portable or personal media, and the information handled by the government administration is sensitive for all of us.

No less a threat to information systems can be human errors, technical failures or malicious attacks. This was the reason for asking: "How do you solve problems related to ICT technologies?" “Fig. 6”. From the results shown, it is noticeable that the percentage of respondents who rely on their own strength to solve problems in the field of ICT has increased. Most employees rely on their knowledge and on friends and colleagues to deal with the problem. Addressing a question to a specialist still maintains its score of around 60%, and delegating responsibility to a specialist has even seen a decrease, although they should be trusted more as they have the knowledge and experience to help resolve complex problems in IT.

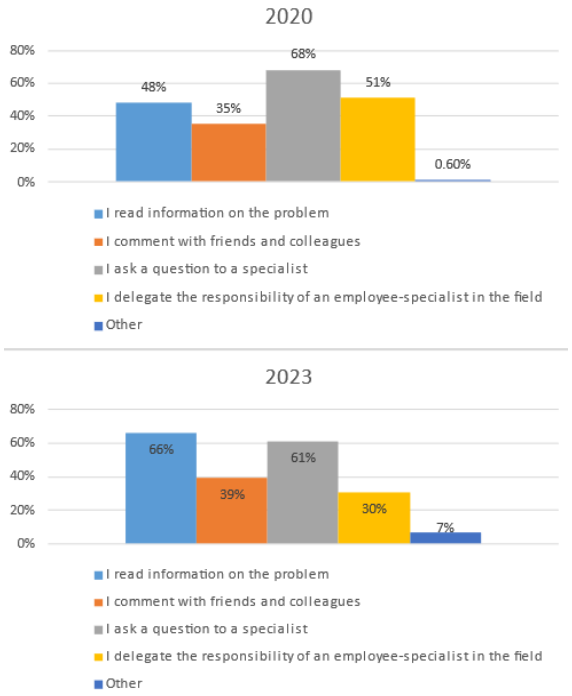


Fig. 6 How do you solve problems related to ICT technologies.

According to an IPA survey to study the level of digital competence of employees in the public administration [14] makes an impression, that employees acquired knowledge during the performance of official duties are twice as many as those who acquired knowledge independently and during on-the-job training (Table 1). Perhaps this also determines the greater confidence in their own abilities than in specialized response.

TABLE 1. DIGITAL COMPETENCE OF PUBLIC ADMINISTRATION EMPLOYEES ACCORDING TO THE IPA REPORTABLE

| | |
|---|---|
| I am self-taught (I have used resources available on the Internet) | 21% |
| The knowledge I have acquired during the work/ work process | 71% |
| The knowledge I have acquired during on-the-job training | 26% |
| The knowledge I have acquired during extracurricular/additional training | 24% |

We asked the surveyed participants “Do you think you have been a victim of a cyberincident/cybercrime?”. Answer "Yes" was written by 8 representatives of the public administration. 6 representatives of the public administration answered "No". The rest indicate that they "don't know". One respondent shared: „It's very possible that my lack of knowledge earlier in life led to a possible data leak - it's entirely possible that something like that happened, but I haven't encountered any consequences for myself so far“.

Overcoming difficulties in IT can provide valuable lessons and opportunity for development, but it often takes much longer. That is why every organization needs to have IT specialists who can not only solve technological problems, but also know the problems that the specific department deals with. This saves time, effort and resources, and manages to increase the efficiency of the organization's work by identifying the most cost-effective solution.

## CONCLUSION

The growing dependence on information and communication technologies in all spheres of human life causes the emergence of vulnerabilities that require proper identification, careful analysis and subsequent removal or limitation. All actors, whether public authorities, private sector representatives or individual citizens, must recognize this shared responsibility, take action to protect themselves and, if necessary, provide a coordinated response to strengthen cyber security.

There is a development of the digital competence of the surveyed public administration employees in the country related to cyber security - prevention, knowledge, protection, application of methods for dealing with cyber threats. From the conducted research, among representatives of the public administration in 2023, compared to that of 2020, there is an increase in the percentage of information security threats that are known. There is also an increase in the values of the used methods and means of protection. At the same time, the percentage of people who do not know the listed protection methods has halved. There is a double increase in 6 out of 7 specified methods of multi-factor authentication used by the respondents. We note that such authentication methods have become a mandatory element when using many of the mobile applications and desktop sites of the banking sector in the country. The increased awareness of the studied group is also considered according to the ways in which they solve problems related to ICT technologies. Respondents have more confidence in their own knowledge to independently solve the problem and/or search for relevant information on it, including by commenting with friends and colleagues. There is a decrease in the percentage of respondents who delegate responsibility to a colleague specialist in the field.

The presented results of the comparative studies in 2020 and 2023 can be used for the adaptation of educational content within the educational process in higher schools, the topics of training for public administration employees, to create the necessary conditions for ethical behavior in the modern working cyber environment.

## ACKNOWLEDGEMENT

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] Department of Economic and Social Affairs, Digital government in the decade of action for sustainable development; UNITED NATIONS New York, 2020. [Online].Available:https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf [Accessed: Feb. 22, 2024].

[2] Report on the state of the administration - 2022. [Online]. Available:https://iisda.government.bg/annual_report_file/623_3190 [Accessed: Feb. 22, 2024].

[3] O. Iliev, R. Yoshinov and G. Tsochev, “Verification of user identity and data security in the context of LMS and LCMS,” Mathematics and Education in Mathematics, Proceedings of the Forty-ninth Spring Conference of the Union of Bulgarian Mathematicians, 2020, pp.144-151.

[4] E. Zhestkova. Subject Information and Educational Environment as Means of Formation of Information and Communication Competence of Future Professionals. Environment. Technology. Resources. Proceedings of the 11th International Scientific and Practical Conference. Volume II, 2017, pp. 180-184. http://dx.doi.org/10.17770/etr2017vol2.2515

[5] R. Trifonov, O. Nakov, S. Manolov, G. Tsochev and G. Pavlova, "Possibilities for Improving the Quality of Cyber Security Education through Application of Artificial Intelligence Methods," International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 2020, pp. 1-4.

[6] Digitalization in training of public administration personnel, © Published by National Institute of Administration on August 2023. [Online]. Available: https://www.ipa.government.bg/sites/default/files/digitalization_in_training_of_public_administration_personnel_2023.pdf [Accessed: Feb. 22, 2024].

[7] L. Coppolino, S. D'Antonio, G. Mazzeo, L. Romano and L. Sgaglione, "How to Protect Public Administration from Cybersecurity Threats: The COMPACT Project," 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), Krakow, Poland, 2018, pp. 573-578.

[8] R. Trifonov and R. Yoshinov, "Some Security Issues of the Governmental Cloud," International Journal of Computers. Vol. 1, 2016, pp. 185- 190.

[9] R Trifonov, S. Manolov, R Yoshinov, G. Tsochev, S Nedev and G. Pavlova, "Operational syber-threat intelligane supported by artificial intelligence methods," Proceedings of the International Conference on Information Technologies (InfoTech-2018), 20-21 September, 2018, pp 1-9.

[10] I, Gaidarski. "Some Aspects of Information Security and Cybersecurity Problem Area," Problems of engineering cybernetics and robotics, Vol. 79, 2023, pp. 55-66. https://doi.org/10.7546/PECR.79.23.03

[11] N. Chehlarova, G. Tsochev, M. Kotseva and R. Miltchev, "Digital Competencies Of Public Administration Employees Related To Cybersecurity," Proc. 12th National Conference with International Participation "Electronica 2021", May 27 - 28, 2021, pp. 1-4.

[12] G. Tsochev and R. Yoshinov, "Research on Cyber-Physical Systems Security," 1st ed., Sofia, Bulgaria: "Education and Knowledge", 2020, p. 258.

[13] T. Tagarev, Krassimir, T. Atanassov, V. Kharchenko and J. Kacprzyk, "Digital Transformation, Cyber Security and Resilience of Modern Societies," 1st ed. Springer Cham, 2021, p. 495, eBook https://doi.org/10.1007/978-3-030-65722-2

[14] Project "Digital Transformation in Education - Digital Competence and Learning", financed by Operational Program "Good Governance", co-financed by the European Union through the European Social Fund. [Online]. Available: https://www.ipa.government.bg/bg/proekt-digitalna-transformaciya-v-obuchenieto-digitalna-kompetentnost-i-uchene [Accessed: Feb. 22, 2024].

## SURVEY

- Your age is: (up to 25; from 26 to 30; from 31 to 35; from 36 to 40; from 41 to 45; from 46 to 50; from 51 to 55; from 55 to 60; over 60)
- You are: (Male; Female; I prefer not to specify)
- After and during the COVID-19 pandemic, did you have to carry out your activity electronically (without direct contact with consumers)? (Yes, for the first time; Yes, but I have done it before electronic; No).
- Are you familiar with (using) any of the listed options for multifactor authentication? (Yes, I use it; I am aware of it, but I do not use it; I am not aware of it) (Face recognition; Voice recognition; Fingerprint; Google Authenticator; Via SMS; Authy; Vein recognition)
- Are you aware of any of the information security threats listed below? (Yes; No) (Viruses, worms and Trojans; Spyware and adware; Identity theft; Lost or stolen devices; Malicious employees; Data misappropriation and theft; Insufficiently informed employees)
- Which of the following 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 IT security)
- How do you solve problems related to ICT technologies? (I read information on the problem; I comment with friends and colleagues, hoping that they have encountered a similar problem; I ask a question to a specialist; I give up the specific problem; I delegate responsibility to a third party; I delegate the responsibility of an employee-specialist in the field; Other)
- Do you think you have been a victim of a cyberincident/cybercrime? (Short answer text).