Artificial intelligence: confidence index in Russia and the world, prospects for implementation

Lyudmila Gruzdeva*
Russian University of Transport (MIIT), 127994 Moscow, Russia

Abstract. Artificial intelligence technologies are being implemented in various fields, replacing the human mind with the help of specially designed algorithms. These systems are able to learn in the course of their functioning, free us from routine work, save time and material resources. The article presents the results of research on trust in breakthrough digital technologies as an important condition for their use, including in social life. There was revealed a high demand for «smart» technologies with an insufficient level of knowledge in this area, lack of interest in professional development. The article identifies the factors causing a negative attitude towards innovation. In the current conditions of the pandemic, a tendency has been revealed of an increase in the need for solutions using artificial intelligence and machine learning technologies, including in ensuring information security.

1 Introduction

The penetration of artificial intelligence (AI) technologies into various spheres of social life can change the social reality not only of the inhabitants of certain technologically most developed countries, but of the whole world. National programs and strategies are developed to develop AI, create benefits, and accelerate innovative change. China was one of the first to approve a new generation of artificial intelligence development plan (2017). In Russia, the «National Strategy for the Development of Artificial Intelligence for the Period up to 2030» was approved in 2019 and the federal project «Artificial Intelligence» was developed. AI technologies imitate the human mind, have the ability to understand, analyze and learn from data using specially designed algorithms. Artificial intelligence systems are able to memorize patterns of human behavior and adapt in accordance with his preferences. One of the examples of artificial intelligence that has entered our lives are “smart” video cameras capable of recognizing documents [1] and identifying a person [2]. Visual navigation systems have found application both in unmanned vehicle control [3] and in algorithms for the movement of humanoid robots [4].

There are many examples of using AI, and at the same time, a number of questions remain relevant:

1) Are we ready for the widespread introduction of artificial intelligence, for the development of technologies that allow machines to reproduce human capabilities much more accurately?

* Corresponding author: docentglm@gmail.com

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).
2) Can AI be entrusted with making decisions related to human life?
3) How will the introduction of AI systems affect the demand for specialists in various fields in the labor market?
4) What role does education play in the formation of the specialists of the future?

2 Materials and methods

The aim of the presented study is to determine the level of trust of residents of different countries in artificial intelligence technologies, as one of the conditions for the use of AI systems in various fields. The analysis was based on statistics that were published in open sources. The tasks were set to determine:
1) the peculiarities of the attitude of Russian citizens to "smart" technologies;
2) factors causing negative attitudes towards AI;
3) possible ways to overcome distrust in innovation.

3 Results

Particular attention on the part of government and commercial organizations to the opinion of citizens towards artificial intelligence is due to the fact that it is the trust of the population that is the most important condition that determines the possibility of using AI technologies in various fields.

One use case for AI is unmanned vehicle control. Errors in unmanned control technology can lead to tragic consequences [3], serious economic and environmental damage. The first serious road traffic accident (RTA) with a "self-propelled" hybrid crossover from Google, in which three employees were injured, occurred in 2015. The accident with a Tesla Model S electric car with the autopilot on, in which the driver died, occurred in May 2016 in the USA. Unfortunately, the list of accidents continues, but experts admit that the introduction of unmanned technologies in transport can lead to a significant reduction in the number of victims of car accidents. Note that Russian experts of the national technology initiative "Autonet" are preparing proposals for amendments to the rules of the road: unmanned vehicles will be able to receive priority on the roads as public transport.

In 2020, the company "Romir", part of the Mile Group, together with the international research community GlobalNR, studied the attitude of citizens of 10 countries to the robotics of road transport: India became the leader in the approval index (71%) of the idea of replacing human drivers with robots, and UK residents were the least supportive of this idea (27%). And only a third of Russians surveyed spoke in favor of the introduction of unmanned technologies. 69% of the world's respondents and 57% of Russians believe that unmanned technologies will become a reality in the next ten years.

A study of the attitude of office workers of American companies to digitalization and robotics, organized by the global developer of solutions in the field of intellectual information processing and linguistics ABBYY, revealed that half of the employees surveyed are ready to transfer some of their functions to machines. At the same time, 1/3 of the respondents do not trust digital "employees": 27% will not delegate any work to artificial intelligence and 32% do not believe that AI could cope with any task better than they.

The majority of Russians surveyed by the All-Russian Public Opinion Research Center have a positive or neutral attitude to the spread of artificial intelligence technologies. Only 29% of respondents were able to define AI, and 38% named the scope of its application. Russian respondents declare a high level of readiness for personal use of services based on AI technologies, primarily public services (68%), leisure and entertainment (54%). Only 54% of Russians surveyed are ready to transfer solutions to everyday tasks to artificial intelligence,
52% want to resort to digital medical care and diagnostics, 44% would like to undergo training using AI technologies.

It should be especially noted that 68% of Russian respondents are not afraid of replacing a person with “smart” technologies in their profession. The study showed that more than 50% of respondents are not interested in advanced training in the field of artificial intelligence since they do not fully understand the essence of technologies and the consequences of their implementation.

The negative attitude of respondents to artificial intelligence is caused by doubts that artificial intelligence systems are capable of performing the tasks assigned to them with the required quality, including in the field of ensuring the security of personal data. People are afraid of violations of personal space, hacking of information systems and theft of personal data.

Analysis of statistical data [5] allowed us to conclude that it is the personnel of companies, including top managers and line managers, who are the main culprits in information security incidents, allowing confidential information to leak (Fig. 1). Cybersecurity Insiders reports that 90% of organizations in the world feel vulnerable to insider attacks. The activity of such attacks is growing with the development and sophistication of digital technologies, as well as an increase in the number of employees with access to confidential data.

To implement information security threats, cybercriminals use malicious software (ransomware, spyware and adware, banking Trojans, etc.) in combination with the exploitation of web vulnerabilities and social engineering methods (Fig. 2), for which fertile soil has been created in a complex epidemiological and the economic situation in the world [6, 7]. The year 2020, amid a pandemic, has changed the principles of interaction between employees of many organizations around the world. In the context of remote work, even the most conservative companies have connected to EDI services (Electronic data interchange) and switched to a full-fledged contactless document exchange.

![Fig. 1. Distribution of leaks by exposure vector, 2017 - 2020.](image)

Phishing is currently the most popular social engineering technique. According to Verizon's 2020 Data Breach Investigations Report (DBIR), in 60% of cases, it was credentials (logins and passwords) that were the targets of attacks, and in 96% of cases, email was used to influence employees of companies and individuals.
The author believes the introduction of artificial intelligence technologies for processing information resources will reduce the number of employees who have access to confidential data and reduce the volume of leaks. AI systems can have vulnerabilities inherent in modern software [8] and be attacked by information security intruders - this must be taken into account. To reduce the possible damage from the successful implementation of threats, you can use the system of an adaptive information protection system [9], algorithms for early detection of malicious activity [10], and currently one of the key areas in protection against cyber attacks is the use of artificial intelligence [11, 12]. According to the Capgemini Research Institute, 64% of organizations with annual revenues of more than $ 1 billion say AI technologies can reduce the cost of detecting and responding to information threats, and about 75% say they have faster response times.

The analysis showed that artificial intelligence technologies are in demand when processing large amounts of data, including information of limited access, and when protecting information systems from cyber attacks.

4 Discussion

Progress has been made in the world towards the creation and application of artificial intelligence technologies, it is a matter of time before AI systems become ubiquitous. With all the advantages of AI, it has an obstacle to development and implementation - people express distrust of new technologies and often do not have the necessary knowledge. Users of information systems often confuse the concepts of artificial intelligence and robotics [13, 14]. Non-AI programs execute a specific sequence of instructions, and AI systems, mimicking the human mind, are able to learn. The education system should help in the formation of competencies in the field of breakthrough digital technologies, such as the Internet of Things, artificial intelligence, virtual reality, wireless communications, augmented reality.

Serious steps have been taken in Russia to ensure confidence in artificial intelligence systems on the part of consumers of their results; the state standard 59276-2020 «Artificial intelligence systems. Methods for ensuring trust. General», which entered into force on March 1, 2021. The maximum number of factors that can lead to a decrease in their reliability must be eliminated in AI systems. Methods for ensuring trust at all stages of the life cycle of
these systems should complement each other, since each of them has both advantages and disadvantages. To improve the efficiency of using AI systems in solving applied problems, on March 1, 2021, the 59277-2020 standard "Artificial intelligence systems. Classification of artificial intelligence systems". It contains the main features of these systems and helps to determine the directions of their standardization. According to the National Strategy for the Development of Artificial Intelligence until 2030, by 2024 the level of participation of Russian specialists in the international exchange of knowledge and their contribution to the creation of open AI libraries should increase significantly. By 2030, software must be developed that uses AI technologies to solve problems in various fields of activity.

5 Conclusion

The study revealed the problems and prospects for the development of artificial intelligence technologies. Analyzed the data of statistical surveys reflecting the attitude of people to "smart" technologies. The presented analysis showed that residents of different countries generally have a positive attitude towards the introduction of artificial intelligence systems. The mistrust is caused by fears for the quality of solving the tasks entrusted to AI, including in the field of information security. The author proposed to transfer functions for processing restricted information to AI systems since it was revealed that it was insiders who were the main channel of data leakage. AI technologies can help protect against cyberattacks and reduce potential damage by reducing the time it takes to detect and respond to information threats.

References

1. Z. A. A. Ibrahim, I. Ferrane, P. Joly, J Image Video Proc. 2011, 537372 (2011) DOI: 10.1155/2011/537372
2. A.T. Kabakus, ADCAIJ: Advances in distributed computing and artificial intelligence journal, 8 (3), 5 (2019) DOI: 10.14201/ADCAIJ201983512
3. M. Cunneen, M. Mullins, F. Murphy, S. Gaines, Applied artificial intelligence 33(3), 267 (2019) DOI: 10.1080/08839514.2018.1560124
4. L. H. Juang, J. S. Zhang, Artificial Intelligence Review 53, 652 (2020) DOI:10.1007/s10462-018-9672-9
5. InfoWatch Analytics Center. https://infowatch.com/analytics
6. Positive Technologies - vulnerability assessment, compliance management and threat analysis solutions. https://www.ptsecurity.com/ww-en/
7. Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition. Wiley, 1235 (2020)
8. T. Habibu, A. E. Sam, International Journal of Advanced Technology and Engineering Exploration 5(45), 243 (2018). DOI: 10.19101/IJATEE.2018.544003
9. L. M. Gruzdeva, Cloud of Science 5(3), 563 (2018)
10. L. M. Gruzdeva, M. Yu. Monakhov, Automation and Remote Control 72, 1075 (2011) DOI: 10.1134/S0005117911050158.
11. N. Lavesson, M. Boldt, P. Davidsson, A. Jacobsson, Knowledge and information systems 26, 285 (2011) DOI: 10.1007/s10115-009-0278-z
12. A. Appice, G. Andresini, D. Malerba, Journal of intelligent information systems 55(101), 1 (2020). DOI: 10.1007/s10844-020-00598-6
13. *Robotics and automation handbooks*, 1st Edition. Edited By Thomas R. Kurfess, Boca Raton, 608 p. (2005). DOI: 10.1201/9781315220352

14. F. Gonzalez, J. Zalewski, Robotics *6*(4), 41 (2017). DOI: 10.3390/robotics6040041