Analysis of Information Risks and Strategies for Protecting Schoolchildren from the Negative Consequences of Digitalization of Education

Kuznetsova V.Y.[1] Azhmukhamedov I.M. Baeva L.V.

Astrakhan State University, Astrakhan, 414056, Russia
[*]Corresponding author. Email: arhelia@bk.ru

ABSTRACT

The article provides a brief overview of the stages of the Russian education digitalization, identifies the main problems associated with this trend, including the relevance of the risks of the digital environment in the field of information security of participants in the educational process. The list of actual risks associated with the violation of confidentiality, integrity, accessibility, authenticity, and non-repudiation of the digital environment users, as well as basic recommendations for their possible minimization are given. The relevance of these risks is confirmed by a survey of teachers conducting their activities in secondary and higher education institutions.

Keywords: *digitalization of education, digital educational environment, information security, protection strategies*

1. INTRODUCTION

The priority project in the field of education "Modern Digital Educational Environment in the Russian Federation" was approved by the Government of the Russian Federation on October 25, 2016 as part of the implementation of the state program "Development of Education" for 2013-2020. Presenting the project at a meeting of the Presidium of the Presidential Council on Strategic Development and Priority Projects, Prime Minister Dmitry Medvedev emphasized that creating a digital educational environment is a strategic state task related to the need to provide the digital economy with qualified personnel [6, 8]. And for their preparation, it is necessary to properly modernize the system of education and training, bring educational programs in line with the needs of the digital economy, widely introduce digital tools of educational activity and integrate them into the information environment, provide the opportunity for citizens to learn according to an individual curriculum throughout their lives - anytime, anywhere.

The priority project "Modern Digital Educational Environment in the Russian Federation" provides for improving the quality and accessibility of education in Russia through the use of online courses at all educational levels [7]. A rather ambitious task was set - by 2025:

the number of students of educational organizations that have attended online courses for formal and non-formal education is 11 million people, of which students of professional educational organizations and educational organizations of higher education should be 5 million people.

On December 13, 2017, Dmitry Medvedev announced the launch of a new priority project - Digital School. This project involves the creation by 2024 of a modern and secure digital educational environment that ensures high quality and accessibility of education of all types and levels, including the transfer of school education "in digital". The website of the national project "Education" says that in 5 years the target model of the digital educational environment will be introduced, which will create digital competency profiles for students, teachers, and administrative staff, design and implement individual curricula, including with the right to set off the results of taking online courses when passing certification activities, automate administrative, managerial and supporting processes; conduct procedures for assessing the quality of education [9].

The implementation of priority projects in the field of education provides for a number of key areas, the development of which is parallel:

- adoption of legal and regulatory acts aimed at the development of online learning. In particular, fixing the status of online courses as equal parts of educational programs;
- Creation of an information resource providing access to online courses on the principle of "one-stop-shop" and combining a number of existing online learning platforms thanks to a unified user authentication system;
- Creation in 2020 of 3500 online courses on secondary, higher and further education programs with the involvement of leading developers, both from government agencies and the business community;
- Formation of the expert system and user assessment of the content of online courses quality;

- Creation of ten Regional centers of competence in the field of online learning;
- Training and education of at least 10,000 teachers and experts in the field of online learning [4].

We focus on the technical component of the project - the so-called digital educational environment, which, according to the "one-stop-shop" principle, will provide students with educational content at all levels of education.

The authors of the project claim that such a system will help students implement the principle of virtual academic mobility in practice, giving them access to quality educational content from leading universities in the country. Moreover, the results of the online course will be counted along with the results of full-time studies [1]. The resource will allow teachers to study the best domestic pedagogical experience and will provide an opportunity to devote more time to practical classes with students and to improve their own qualifications. For people seeking to acquire new knowledge or update their skills, it will provide convenient and high-quality service. Employers will be able to directly express their wishes for training content in order to bring it in line with the requirements of the labor market. For educational platforms and creators of online courses, the "one-stop-shop" resource will provide a unique opportunity to expand the audience, improve the quality of your product, and offer a flexible and convenient analytics tool.

As a result of a competitive selection conducted by the Ministry of Education and Science of the Russian Federation, the St. Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University) became the executor of the project to create such an information resource.

1.1. The problem of creating a safe educational environment

According to the priority state project, the educational environment should be safe for all participants in the educational process, as well as ensure high quality and accessibility of education of all types and levels. At the same time, the introduction of a single educational system for all of itself poses a number of risks that threaten the safety of participants in educational activities (students, teachers) in various aspects of their life (for example, the threat of weakening social and communication skills, poor physical and psycho-emotional health, etc.) [10]. Among other things, there are information risks associated with the safety of the educational process in the digital economy [2].

We believe that the digitalization of the education and upbringing system in the modern world and in Russia is designed not only to adapt a person to life in the information society, but also to create conditions for his personal development, safe communication and intellectual and growth. Currently, different countries have already accumulated significant experience in the digitalization of education and training, identified growth points and bottlenecks. The main attention was initially associated with the creation of technological conditions for digital open education, at the present stage, society faced the need to ensure the safety of the student (including information security) and create a sustainable educational digital environment [3].

2. BACKGROUND

In connection with all of the above, analysis and classification of information risks associated with the implementation and realization of a unified digital educational environment, from the point of view of the main information security services are: confidentiality, integrity, accessibility, authenticity and non-repudiation become relevant.

2.1. Confidentiality

According to the federal law "On Information, Information Technologies and Information Protection", confidentiality is a requirement for a person who has access to certain information to not transfer such information to third parties without the consent of its owner. Confidentiality includes procedures and measures to prevent the disclosure of information by illegitimate users. First of all, the confidential information within the educational process can be attributed to the personal data of the digital environment participants:

- Full Name;
- Date of Birth;
- Address of registration and residence, contact phones, email addresses;
- Passport data or birth certificate data.

This list can be adjusted depending on the requirements of an educational institution or a single educational platform.

In addition, based on the definition established by the Federal Law "On Personal Data", biometric personal data include physiological data (fingerprints, iris, DNA tests, height, weight and others), as well as other physiological or biological characteristics of a person, including the image of a person (photograph and video), which allow to establish his identity and can be used to establish the identity of the subject. Photos of participants in the educational process are supposed to be used in the implementation of digital learning as avatars of accounts.

Risks of violation of confidentiality include the illegitimate distribution of personal information of participants in the educational process, for example, contact details, photographs, as well as assessments of individual tasks performed. The dissemination of personal data can lead to problems not only in the educational system, but also beyond, for example, when intruders can use the personal data of a child for theft or bullying [5].

Based on the foregoing, it can be said that the digital learning system should in all possible ways ensure the confidentiality of the processed information, including in accordance with current legislation in the field of personal data protection.

Decree of the Government of the Russian Federation No. 1119, adopted on November 1, 2012, approved the requirements that apply to the protection of personal data (PD) when they are processed in information systems. From the point of view of processing personal data, the digital environment will also be ISPD, therefore protection should be provided in accordance with the requirements of the resolution.

According to the requirements of the above normative act, DE is characterized by 3 types of actual threats and 3 level of security (Table 1).

Table 1 Determination of the security level of ISPD of the digital environment

Type of PD	Subject category	Number of subjects	Type of actual threats		
			1 type	2 type	**3 type**
Special	Not employees	More than 100,000	PL 1	PL 1	PL 2
		Less than 100,000	PL 1	PL 2	PL 3
	Staff	Any	PL 1	PL 2	PL 3
Biometric	**Any**	**Any**	PL 1	PL 2	**PL 3**
Other	Not employees	More than 100,000	PL 1	PL 2	PL 3
		Less than 100,000	PL 1	PL 3	PL 4
	Staff	Any	PL 1	PL 3	PL 4
Publicly available	Not employees	More than 100,000	PL 2	PL 2	PL 4
		Less than 100,000	PL 2	PL 3	PL 4
	Staff	Any	PL 2	PL 3	PL 4

To ensure the 3rd level of security, technical protection of the premises in which the ISPD elements are located, including the intra-object mode with limited access, is required.

The measures to ensure the 3rd level of security of personal data implemented within the framework of the personal data protection system taking into account current threats to the security of personal data and applied information technologies include:

- identification and authentication of access subjects and access objects;
- access control of access subjects to access objects;
- protection of computer storage media on which personal data are stored and (or) processed;
- registration of security events;
- antivirus protection;
- control (analysis) of the security of personal data;
- protection of virtualization environment;
- protection of technical equipment;
- protection of ISPD, its means, communication systems and data transmission;
- configuration management of ISPD and personal data protection system.

These measures are relevant not only to protect personal data, but also in general to ensure the confidentiality of information stored in the system.

2.2. Integrity

This term in the field of information technology means that data has undergone a change in the performance of any operation on it, whether it be transmission, storage or display.

Given the specifics of the mechanisms used to ensure data integrity, three aspects of this concept can be distinguished.

– **Correctness**. It consists in the absence of logical errors in the structure and errors in the content (in values) of the data during their processing.

– **Absence of distortion**. It consists in the absence of data falsification or errors in the data during their transmission in communication lines, as well as during storage.

– **Invariance**. It consists of the identity of the data to a specific standard.

As part of the implementation of a unified digital educational environment, this information security service is relevant no less than confidentiality for several reasons.

First of all, the modification and distortion of educational content is unacceptable, unless the teacher or system administrator legitimately makes corrections to the teaching material in order to clarify, correct errors or update the content in connection with changes in the educational standard or other legal acts.

Secondly, educational content should comply with the requirements of the regulatory framework, i.e. correspond to the standard, discrepancies and approximate information are unacceptable.

Thirdly, the absence of logical errors in the structure of not only educational content or the entire course, but also the digital educational environment itself is critically important. In case there are violations in the logic of the educational platform, technical problems, inaccessibility of educational materials, courses or supporting sections of the environment are possible.

The main methods for ensuring the integrity of information during storage in information systems (which is the digital environment) are:

1) ensuring fault tolerance (redundancy, duplication, mirroring of equipment and data).

Redundancy and duplication perform the same function in providing fault tolerance - the creation of spare system elements in case the main system is not able to carry out the work in full. For example, in case of violations in the operation of the main system, a copy of the educational platform is created, and the educational process is temporarily or constantly transferred to it.

2) secure recovery (backup and electronic archiving of information).

This method includes the creation of various kinds of backups for the timely recovery of damaged data or the entire educational platform as a whole. Storage of the created backups should be provided in separate storages, which are not connected in any way with the main system.

3) ensuring secure data transfer using cryptographic protection tools (encryption, hashing, electronic digital signature).

To avoid violation of the integrity of the data during their transmission, for example, in the case when the teacher makes changes to the content of the training course located on the educational platform, the above cryptographic protection tools are used to detect data corruption. If it is revealed that the data has been corrupted after the transfer, no changes will be made to the existing data system.

2.3. Availability

According to the standard R 50.1.053-2005, this term refers to the state of information (resources of an automated information system), in which subjects with access rights can implement them freely. Access rights include: the right to read, modify, store, copy, destroy information, as well as the right to change, use, destroy resources.

Violation of accessibility is the creation of such conditions under which access to information will be either blocked or possible for a time that does not ensure the fulfillment of certain goals. For example, one of the most common methods of accessibility violation is loading an information system (loading network bandwidth, processing capabilities of processors or RAM - DDoS attack) or introducing malicious code into the system. Natural disasters are also dangerous - fires, floods, earthquakes, hurricanes. According to statistics, these sources of threats, taking into account power outages, account for 13% of losses caused to information systems

Ensuring the accessibility of the digital educational environment is an urgent and fundamentally important task, because even short-term blocking of educational content violates the basic principle of education - the principle of accessibility of education. In addition, the threat of accessibility violates the integrity of the educational process, which consists of 4 interconnected components:

- The process of mastering and designing the content of training and materials base;
- the interaction of teachers and students in the educational process, as part of a holistic pedagogical process;
- personal interaction of teachers with pupils;
- independent learning lessons by students.

The loss of any element leads to a collapse in the effectiveness of the educational process and significantly reduces the effectiveness of training.

The main methods for ensuring the availability of data during storage in automated systems are uninterruptible power systems, as well as backup and duplication of capacities, so that in case of threats, the system is restored in a timely manner.

2.4. Non-repudiation

Otherwise, this security service is called non-repudiation of authorship of information, as well as the fact of its sending or receiving.

The risks of breach of non-repudiation include the ability to refuse the fact of the creation, transmission and receipt of information. An example is the refusal to send an insulting letter or the refusal to deliver a training exam late.

In order to minimize the risk of breach of non-repudiation in a digital educational environment, a non-repudiation mechanism should be implemented that will ensure the collection, processing, accessibility, and recognition of incontrovertibility of evidence regarding the declared event or action in order to resolve disputes about the event or event that has occurred or not occurred.

The procedure for ensuring non-repudiation includes four phases: the formation of evidence, delivery, storage and retrieval, verification (confirmation of authenticity) of the evidence and resolution of the dispute.

2.5. Authenticity

The term "authenticity" means the ability to uniquely identify the author or source of information. Some other sources refer to this information service as "authenticity".

Authentic information is in respect of which it is proved:

– it was not subject to change;

– it was created or sent by the user who is specified as the creator or sender;

– it was created or sent exactly at the time indicated in it.

Also, this risk implies the ability of the subject to impersonate another user. This subject can be both a participant in the educational platform and an external attacker. The result of such activities, for example, can be unauthorized changes in content, fraudulent actions in obtaining an education in order to pass an examination for a student, making changes to a point-rating system, etc. Personal data may also be compromised (violation of confidentiality) or organized the distribution of illegal content, offensive messages on behalf of other people.

Authenticity is inextricably linked to the identification and authentication of users. Authentication can be carried out by various methods and means. Currently, automated systems use three main authentication methods based on the following criteria:

1) Password protection

It is implemented by authentication software used in most operating systems, database management systems, teleprocessing monitors, network packets. Each registered user is given a personal password, which he should keep secret and enter into the system each time he accesses it. A special program compares the entered password with the standard stored in the memory, and when the passwords match, the user's request is accepted for execution.

2) Use of individual media.

As an object that a user has, identification cards (IDs) are used, on which data are applied that personify the user: a personal identification number, a special cipher or code, etc. This data is entered on the card in encrypted form, and the encryption key can be an additional identifying parameter, since it can only be known to the user, is entered by him every time he accesses the system and is destroyed immediately after use.

3) the use of physiological signs of legal users of the system (retina scan, fingerprint, Face-ID).

There are enough physiological signs that uniquely indicate a specific person. These include: foot and hand prints, teeth, enzymes, respiratory dynamics, facial features, etc. For authentication of terminal users of automated systems, fingerprints, hand geometry, voice, personal signature are considered the most acceptable. When directly comparing images, the authentication device determines the optical ratio of the two images and generates a signal that determines the degree of coincidence of the prints. Comparison of prints is usually performed directly at the installation site. The transfer of the fingerprint image through communication channels is not used due to its complexity, high cost and the need for additional protection of these channels.

It should be noted that in the case of non-authentication, all the authentication methods considered should be delayed before serving the next request. This is necessary to reduce the threat of identifying identifiers (especially passwords) in automatic mode. Moreover, all unsuccessful attempts to gain access should be recorded in order to ensure effective supervision (control) of the security of the system.

In connection with the foregoing, it becomes optimal to use several authentication methods, including two-factor authentication.

3. RESULTS OF ANONYMOUS QUESTIONNAIRE

An assessment of the relevance of the stated risks is impossible without taking into account the views of the participants in the educational process themselves. In this regard, a survey was conducted of teachers of schools, colleges and universities, the results of which were statistically processed.

The calculation of a representative sample is based on a formula that takes into account the level of confidence in the results obtained in the study, as well as the permissible error margin:

$$\mathrm{V_{RS}} = \frac{\frac{\mathrm{Z^2 \cdot p(1\text{-}p)}}{\mathrm{e^2}}}{1+\left(\frac{\mathrm{Z^2 \cdot p(1\text{-}p)}}{\mathrm{e^2 N}}\right)}, \quad (1)$$

where *N* is the size of the general population, e is the margin of error in the form of a decimal fraction, *Z* is the confidence level (*Z*-score), *p* is the part of the sample of interest percentage to the researcher that showed a certain behavior during previous tests (also as a decimal fraction). In the initial study, the recommended value is *p* = 0.5.

The margin of error is a percentage value that shows how likely the opinions and sample behavior deviate from the opinions and behavior of the total population. The level of confidence indicates how reliable the results are; generally accepted standards used by researchers: 90%, 95% and 99% (in fact, a 95% confidence level means that if you repeat the same study under the same conditions 100 times, 95 times out of 100, the results will be within the margin of error). When determining the sample size, a *Z*-score of the confidence level is used - a measure of the standard deviation of a certain fraction from the average value (1.65; 1.96 or 2.58, respectively).

The composition of a representative sample is determined on the basis of statistical data and methodological recommendations on the organization of sample observations of the Federal State Statistics Service (Rosstat). According to its data for 2018, in the Russian Federation there are 1.504 million teachers (schools, colleges, universities).

$$V_{RS} = \frac{\frac{1{,}96^2 \cdot 0{,}5(1-0{,}5)}{0{,}05^2}}{1+\left(\frac{1{,}96^2 \cdot 0{,}5(1-0{,}5)}{0{,}05^2 \cdot 1711000}\right)} = 384, \quad (2)$$

Thus, the volume of a representative sample was calculated, which is equal to 384 respondents. It is this number that was surveyed as a result of the survey. The questionnaire took place in paper and electronic form: paper questionnaires were distributed among teachers of secondary schools in Astrakhan and teachers of Astrakhan State University, an electronic questionnaire implemented in the Google.Forms service was posted in a closed pedagogical community on the social network "Vk.com".

The above risks were suggested to respondents to select the most relevant when implementing a digital educational environment. The survey results are shown in Figure 1.

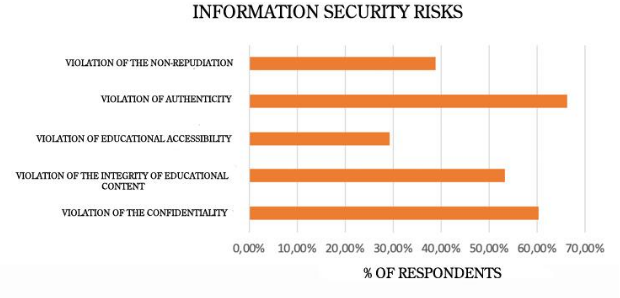

Figure 1 Bar chart of the opinions of the surveyed teachers on the relevance of information security risks

The diagram clearly shows that the greatest concerns among the pedagogical community are caused by the risks of violation of confidentiality, integrity, and authenticity in the implementation of the digital educational environment (more than half of the respondents noted these answer options when participating in the questionnaire). At the same time, the greatest number of responses received a risk associated with authenticity. It is noteworthy that this risk is also most relevant for the implementation of the classical class-lesson form of education (the danger that one student will write a test for another or "forge" the marks in the teacher’s journal), which suggests that the risks of the digital educational environment are the same sources as classical education.

4. CONCLUSION

Informatization of education plays an important role in improving the quality and accessibility of education. The introduction of new technologies in the learning process allows, along with traditional teaching materials, to use modern electronic means to support and support the educational process. However, the transition to digital education poses threats that are caused by the very fact of organizing educational activities in digital format - information risks, and they cannot be ignored. When implementing this system, it is necessary to carefully evaluate the consequences of this type of training and adopt an optimal protection strategy against the threats it causes.

ACKNOWLEDGMENT

This article was supported by a grant from the Russian Foundation for Basic Research, project No. 19-29-14007 mk "Assessing the impact of digitalization of educational and social space on a person and developing a system of a safe communicative and educational environment".

REFERENCES

[1] Abdrahmanova G.I. Kovaleva G.G. O chem govoryat cifry. - Narodnoe obrazovanie. - 2011. - № 10. - s. 48-51

[2] Aetdinova R.R. Analiz i klassifikaciya riskov cifrovizacii obrazovaniya // Materialy XVII mezhdunarodnoj konferencii «Obrazovanie cherez vsyu zhizn': nepreryvnoe obrazovanie v interesah ustojchivogo razvitiya», pod redakciej V. P. Galenko, N. A. Lobanova. Izdatel'stvo: Sankt-Peterburgskij gosudarstvennyj ekonomicheskij universitet. Sankt-Peterburg, 2019. S.145-148.

[3] Baeva L.V. Sociokul'turnye i filosofskie problemy razvitiya informacionnogo obshchestva. Izd.- Astrahanskij gosudarstvennyj universitet, 2019. – 137 s.

[4] Zlenko N.S. Pochemu obrazovanie v Rossii nuzhdaetsya v cifrovizacii? // sbornik statej po materialam LXX studencheskoj mezhdunarodnoj nauchno-prakticheskoj konferencii. Moskva, 2020. S. 72-77.

[5] Majkulov ZH. ZH. Prestupleniya protiv detej s ispol'zovaniem Interneta // Nauchno-metodicheskij elektronnyj zhurnal «Koncept». – 2017. – T. 39. – S. 2636–2640. – Rezhim dostupa: http://e-koncept.ru/2017/970854.htm.

[6] Markelov K.A., Brumshtejn YU.M., Azhmuhamedov I.M. Analiz sushchestvuyushchih i perspektivnyh napravlenij ispol'zovaniya distancionnyh obrazovatel'nyh tekhnologij v rossijskih regional'nyh gosudarstvennyh vuzah // Distancionnye obrazovatel'nye tekhnologii. Materialy IV Vserossijskoj nauchno-prakticheskoj konferencii (s mezhdunarodnym uchastiem), 2019.

[7] Opisanie proekta «Sovremennaya cifrovaya obrazovatel'naya sreda». Rezhim dostupa: http://neorusedu.ru/about (data obrashcheniya 20.01.2020)

[8] Prioritetnyj proekt «Sovremennaya cifrovaya obrazovatel'naya sreda v Rossijskoj Federacii», utverzhdennyj Prezidiumom Soveta pri Prezidente RF po strategicheskomu razvitiyu i prioritetnym proektam (protokol ot 25 oktyabrya 2016 g. № 9) // Konsul'tant. Rezhim dostupa: http://www.consultant.ru/ (data obrashcheniya 20.01.2020)

[9] Prioritetnyj proekt «Cifrovaya shkola». Rezhim dostupa: http://government.ru/projects/selection/693/30822/ (data obrashcheniya 20.01.2020)

[10] Bilyalova, A., Salimova, D., Zelenina, T.: Digital transformation in education. In: Antipova, T. (ed.) Integrated Science in Digital Age, ICIS 2019. LNNS, vol. 78. Springer, Cham (2020)