Galactica Media: Journal of Media Studies. 2021. No 2 | ISSN: 2658-7734
Media Safety & Security | Doi: https://doi.org/10.46539/gmd.v3i2.161

THE "BLACK SWAN" OF COVID-19 AND THE SECURITY ISSUES IN DIGITAL LEARNING

Liudmila V. Baeva

Astrakhan state University. Astrakhan, Russia. Email: baevaludmila[at]mail.ru

Abstract

The social security problems come to the fore as the relationships between individuals, society and modern technologies become more and more complicated. In the context of the pandemic social security issues turned out to be decisive for the education system, the transformation of which caused significant difficulties. The article covers the topic of the security of digital education and focuses on theoretical concepts as well as on the analysis of practical cases found in the media. The author analyzes the experience of educational organizations and education management institutions in the area of protection against risks in the information environment, and identifies the most successful approaches. As a result, the conclusion is made that it is necessary to create a system of safe information and communication environment that should be designed to ensure the rights and quality of life of individuals in the context of the digital transformation of educational and upbringing processes.

Keywords

electronic culture; media environment; digital education; social security; cybersecurity threats; cyberbullying; COVID-19

Galactica Media: Journal of Media Studies. 2021. No 2 | ISSN: 2658-7734
Медиабезопасность | Doi: https://doi.org/10.46539/gmd.v3i2.161

«ЧЁРНЫЙ ЛЕБЕДЬ» COVID-19 И ПРОБЛЕМЫ БЕЗОПАСНОСТИ ЦИФРОВОГО ОБУЧЕНИЯ

Баева Людмила Владимировна

Астраханский государственный университет. Астрахань, Россия. Email: baevaludmila[at]mail.ru

Аннотация

Проблемы социальной безопасности выходят на первый план по мере усложнения связей человека, общества и современных технологий. В условиях пандемии вопросы социальной безопасности оказались определяющими и для системы образования, трансформация которой вызвала значительные трудности. Статья посвящена вопросам безопасности цифрового образования, как концептуальным теоретическим понятиям, так и анализу практических кейсов в медиасреде. Проведено изучение опыта образовательных организаций и учреждений по управлению образованием в сфере защиты от рисков в информационной среде, выявлены наиболее успешные подходы. В результате сделан вывод о необходимости создания системы безопасной информационной и коммуникационной среды, призванной обеспечить права и качество жизни граждан в условиях цифровой трансформации образовательного и воспитательного процессов.

Ключевые слова

электронная культура; медисреда; цифровое образование; социальная безопасность; киберугрозы; кибербуллинг; COVID-19

INTRODUCTION

The year 2020 turned out to be linked with a new challenge for the world, the *COVID-19* pandemic, like M. *Taleb's "black swan"* that became a point of no return for society (Taleb, 2015). Unpredictable, uncontrollable, covering almost all of humanity, changing the life of everyone, it forced to revise many norms and orders that define life. First of all, the new restrictions turned out to be related to communication and personal intercourse, which led to the need to switch to remote work and a distance learning format. Interpersonal relationships have almost completely moved to the media environment, namely, to social media, educational portals, electronic libraries, etc. Under these conditions, information technologies have created the opportunity to carry out continuous working activity for many sectors of economy, although a number of them, unfortunately, were victims of a lockdown. Education in these unprecedented circumstances was transferred to distance form of work in various forms, and remains so for many countries and large cities. The pandemic has become a powerful challenge to social resilience, showing that human life is still subject to high risks, and economic growth and well-being are not guaranteed even in developed countries.

The education system was already partly on the path of digital transformation even before 2020, but it was a "small island" in a sea of traditional learning. Digital education has become common practice in 2020. After the digital turn, the education system in schools and universities found itself in an unexampled experiment, which made it possible to draw important analytical conclusions about the impact of digitalization on education. The digitalization of education in the context of the pandemic has made it possible to maintain the continuity of education at all levels. However, the problem of information inequality and access to resources has still arisen. This especially affected large families of low-income citizens, where not every child had their own gadget for study, as well as families living in remote areas – due to the problems with high-speed Internet. The digital gap has thereby increased social exclusion, when a number of citizens and their children did not have the same chances to use the offered opportunities. At the same time, the digitalization of education has revealed not only the issues of the growing digital disparity, but a whole range of other problems related to social security. It is obvious that digital learning turned from a temporary measure to a new social trend, intention, irreversible action, and for this reason it became necessary to study its possible social consequences and the nature of its impact on a person. Having ensured the safety of subjects in the context of the spread of morbidity, digital learning

was transferred to a special virtual communication environment that has its own characteristics and risks connected, on the one hand, with a high level of cybersecurity threats, and on the other, characterized by high pluralism and the absence of rigid regulatory boundaries. The purpose of our research is to identify and characterize the social problems of digital education related to personal safety and to study practices providing such problems prevention. To do this, our study used the theory of electronic culture, the theory of social security and risks, as well as the method of focus group research, elements of content analysis and analysis of media cases.

DIGITAL EDUCATION AS AN ELEMENT OF ELECTRONIC CULTURE

In the present-day information society, a special type of culture has formed, into which the human life world and the environment around it are gradually shifting – that is, the world of electronic, digital, online or cyber culture, a kind of "third nature" with many new phenomena and processes. In the most general sense, electronic culture (online culture, e-culture) is considered by us as a sphere of human activity and its results related to the creation of electronic analogues of spiritual and material objects, as well as virtual spaces, processes and phenomena themselves (Baeva, 2013; 2014). In a narrower sense, electronic culture is a set of results of creativity and communication of people under the introduction of IT innovations, which is characterized by the creation of a single information space, a virtual form of expression, distance technology, liberal content, including both virtual phenomena proper and virtual analogues of real objects.

Of note is that the structure of electronic culture is heterogeneous, it includes such basic types of objects as:

1) digitized analogues of the manifestations of non-digital culture: digital libraries, digital data, video and photo archives, digital copies of works of art, digital education, electronic media, electronic governmental and commercial services, online banks, currencies, and much more. The function of such digital analogues of cultural objects is their adaptation to the conditions of the information age, increasing the convenience of their use and transmission for humans;
2) manifestations of culture, electronic in form and content, that had no analogues in pre-digital culture, as the Internet, artificial intelligence, big data, social media, the Internet of things, etc.;
3) information technologies, networks, systems, resources related to the creation and management of data, knowledge, communication channels, etc.

Electronic culture and its phenomena have a special nature, being a synthesis of knowledge and information phenomena. The characteristic features of objects of the first and second types of electronic culture are as follows:

- freedom of access, openness for members of the information society (possessing the necessary resources and competencies);
- distance, real remotedness from the knowing agent;
- interactivity, the ability to participate in the information content forming from any point in the information community;
- liberality, descriptiveness, absence of rigid rules, and norms (including ethical ones);
- eclecticism, diversity of content, coexistence of different streams of information, of styles, genres, and trends;
- virtuality as existence in an artificially created reality;
- fragmentation, mosaic expression, dominance of the visual over the semantic;
- innovativeness, existence through the introduction and constant updating of scientific developments (especially in electronic art and electronic communication);
- entertaining and playful character used both in traditional spheres (learning, recreation, leisure) and in others (online advertising, -trade, -banks, etc.).

Objects of electronic culture do not just replace the originals; they largely develop them, supplement them with new opportunities, and make them more accessible, interactive, and widespread. They become not only a doubling of "living" culture as its digital copy, but also acquire their own ontological status, having special parameters and characteristics that are not inherent in the phenomena of material culture or phenomena of consciousness. In the field of virtual interaction in electronic culture, its own communities, rules, etiquette, language are formed, developing rapidly, sometimes in opposition to the existing reality, sometimes by analogy with it. Electronic culture acts not just as the "environment" for a contemporary person, but as his/her existence, where new problems of living in a digital society arise: blurring of the boundaries of real and virtual; questioning the trust in virtual communication with the digital analogue of the Other; deformation of cultural, as well as social identity and the formation of digital and network identities; new forms of alienation, escapism, digital runaway from reality;

manipulating consciousness and behavior of an individual in the information space; the formation of new types of unfreedom, dependence on virtual objects and processes; replacement of individuality with cyber-corporeality; existential security in a digital society, etc.

Digital education, based on e-learning, has become one of the most important components of e-culture, contributing to the adaptation of citizens to life in its conditions. Digital education has signs and features inherent to the objects of electronic culture in general, many of which complement and develop its capabilities (accessibility, openness, interactivity, game elements), but a number of them may also have a potentially risky nature (openness, interactivity, lack of regulatory rules, control from any place, etc.).

Social and existential problems and security risks peculiar of the e-culture turn out to be more or less inherent in digital education. And as digital education begins to play an increasing role for an increasing number of citizens, determining the life of the present and future generations of children and youth, the study of the parameters of its safety and social risks becomes a necessary step for its development and humanitarian expertise.

ASSESSMENT OF THE IMPACT OF DIGITAL EDUCATION ON HUMANS

The issues of assessing the impact of digital technologies on the education system and on a person from a security standpoint have become more and more relevant since the beginning of the 21st century, as such learning is increasingly used. The researchers note that digital learning makes it possible to widely use the possibilities of individualization, interactivity, visualization, gamification of training; it creates ample opportunities for managing education based on artificial intelligence, processing big data on learning outcomes and problems. The positive aspects of the impact of digital learning on a person include the following:

• The digital learning process (DL) is activated on the two sides: both the teacher and the student (student) act as creators of information, participants in the communication process, acquire knowledge and skills in a single digital environment. Digital learning involves the development of skills for self-study, independence, initiative, self-control, etc.

• DL assumes individualization of training, flexible adjustment of the curriculum, the speed of mastering it, specific methods of online or offline learning in accordance with the age group, psychological type of personality, etc. (Gaskell, 2009).

• DL is characterized by high innovation, dynamism of changes, updating of content, interfaces, software based on the constant implementa-

tion of the achievements of the scientific and technological revolution in teaching practice.

- DL allows students to receive constantly updated, multilateral, and not only bound by unambiguous interpretation, information about the object of study. Speed, breadth of coverage, democratic access, the ability to learn more – all this characterizes the features of the modern receipt of information by students at school or university.
- Informatization visualizes information, makes the learning process effective for working with different age and other groups. (Ghosh, Nath, Agarwal & Nath, 2012)
- DL is based on the principle of interactivity, which fosters students' interest through the co-creation of information, opportunity and consideration of continuous feedback.
- DL makes the learning process as transparent as possible, verifiable from the outside, reduces subjectivity in estimating students by the teacher, and possible "pressure" on the student's personality.
- DL allows people to study on-the-job, with the family, saying away from the educational institution or having health difficulties, or hard access to receive a classical education.
- Being highly democratic and widespread, this makes DE the most popular for generations from 30+ to 70+, as well as for the development of forms of additional education (MOOC) (Thompson, 2012).

At the same time, researchers are identifying the highest risk factors associated with the use of online learning.

Even before the widespread use of online learning in 2020, the risks of the formation of addictive behavior were identified; for example, a study by Y. Alghamdi showed that the introduction of educational digital technologies at a young age can lead children to social isolation, cause depression, serious mental and physical illnesses and disorders (Alghamdi, 2016). In addition, emerging threats to the health of students were noted due to lack of physical activity, prolonged exposure to the screen, stress on vision, musculoskeletal system, etc. (Mustafaoğlu, 2018). A number of studies identified significant problems and risks in the use of digital learning connected with a decrease in motivation to study (Strekalova, 2019), with a decrease in interpersonal communication skills (Karpova, 2016), the formation of mental disorders in behavior: from apathy to aggression (Schneider & Symaniuk,

2017; Panchenko, Mukhametzyanova & Khairutdinov, 2019), weakening of cognitive functions (Khrapov, 2020). N. S. Ilyushenko, considering the risks of a digital turn in education, distinguished the following: additional study and workload for students and teachers, large time costs for creating a digital educational product and its rapid obsolescence with a loss in the quality of content, a decrease in the quality of formed skills that develop only in "face-to-face" communication as well as problems of digital security and digital discrimination (2019). In general it should be noted that studies on the impact of digital education on a person from a security standpoint until 2020 were mostly episodic. Since the task of digital transformation of education has today been set by the government of many countries, including Russia, it becomes necessary both to perform step-by-step consistent movement in this direction, and to assess possible risks and threats as one of the priorities (Semenov, 2019). Year 2020 has accelerated the digital turn in education, while also highlighting some of its major challenges. These transformations caused a significant social effect; in many aspects they were accompanied by negative assessments of students and parents, which forces researchers to more carefully analyze the associated risks and pay the most serious attention to human safety issues in the digital learning environment.

ASSESSMENT OF RISKS OF DIGITALIZATION OF EDUCATION

Year 2020 was a turning point both for the world as a whole and for the education system, which was forcedly transferred to a distance format, making it possible to reduce the threat of the spread of coronavirus infection. Year 2020 was a turning point both for the world as a whole and for the education system, which was forcedly transferred to a distance format, making it possible to reduce the threat of the spread of coronavirus infection. This process was uneven and showed that a significant part of schools and universities were not ready for such a transformation. At the same time, the education system, in the context of self-organization, rapidly began to adapt to new conditions, and by the second semester considerable experience had already been accumulated in methodical, organizational and also educational activities, as well as, in some cases, in the field of psychological and social support for the students.

As the education process became conditioned by the peculiarities of virtual communication and shifted to the digital environment, certain social threats also emerged. The practice of a general transition to online learning showed the crucial threats that were associated with a violation of personal security and human rights in the digital environment, with the possibility of cyberattacks, transmission of classified information, the spread of fakes, cyber

fraud, which in these conditions receive new impulses and forms of manifestation.

At the end of 2019-2020, within the framework of the project "Assessing the impact of digitalization of education on a person" at the Astrakhan State University, two mass surveys and a series of focus groups from teachers of schools and colleges in Astrakhan were organized and conducted to estimate the problems encountered during the transition to distance learning format. Surveys on information security issues were conducted in two waves, the first in November-December 2019 and the second in the context of the transition to digital learning in self-isolation mode in April 2020 (the sample consisted of 400 respondents, including teachers of schools and colleges in Astrakhan and a number of districts of Astrakhan region). The results of the first wave of the survey (November-December 2019), in which 400 teachers were interviewed, showed that teachers put in the first place the problems of violation of authenticity and confidentiality among the most pressing risks. After the ntroduction of the self-isolation regime and the transition of schools to digital education, the situation changed dramatically: after the massive transition to a digital learning environment, teachers put digital inequality (lack of availability of technical resources) and violation of the integrity of educational content (more than 70% of respondents) in the first places among the risks. Violations of educational content have been linked to a variety of factors, from fakes to cyberattacks. The results of the conducted surveys showed that the greatest fears among the pedagogical community in the implementation of the digital educational environment (DEE) in the information sphere are caused by the risks of violation of confidentiality, content integrity and authenticity (over half of the respondents). The teachers also noted the risks in the legal sphere: the increase in cases of plagiarism among students, violation of the copyright of teachers for methodological or didactic materials, a decrease in the level of unique educational material (Azhmukhamedov & Kuznetsova, 2020, p. 10).

A series of focus groups with school teachers aimed at examining the main difficulties and risks encountered in the course of digitalization was held in June 2020. Three focused group interviews were organized, homogeneous on two grounds: the professional affiliation of the respondents and the use of digital educational technologies in their activities. During the processing of the results, such a method as mind mapping was used; consequently, a mental map of teachers' opinions regarding the process of digitalization of education was drawn.

The teachers identified the various risks they faced in the digital learning environment and in the organization of educational activities:

1) problems of affordable internet connection and personal gadgets;

2) introduction of undesirable, "adult" content into educational resources, general problems of information security violation;
3) significant problems with the organization of learning in the digital environment of primary and secondary schoolchildren who are not able to organize their workspace on their own;
4) general decrease in learning outcomes, weakening of motivation to study, concentration of attention during online classes, deterioration in memorizing the material (possible reasons are associated with the loss of motor skills in writing, as well as an increase in the information flow), significant difficulties in the assimilation of educational material in several subjects;
5) lack of teaching materials for learning in a digital environment;
6) the risks of losing the opportunity to develop creative skills of students who can borrow ready-made samples in the digital environment;
7) physical health and safety issues. Students have a dramatic increase in "screen time", which affects vision, the musculoskeletal system, the nervous system, thus disrupting the healthy lifestyle of the student (and the teacher);
8) possible risks in the field of socialization and adaptation of students, weakening and even loss of the upbringing function of education associated with the transmission of values.

The results of surveys and focus groups were studied and formed the basis of the cluster theory of digitalization risks (Baeva, Khrapov, Azhmukhamedov, Grigoriev & Kuznetsova, 2020).

The following main risk-generating clusters were identified: informational, cognitive, social, vital and addictive.

I. Information cluster is associated with possible threats and risks from negative information impact in the cyber environment.

The main parameters of information threats to the educational process associated with the implementation and realization of a unified digital educational environment, from the point of view of the main information security services, are: threats of violation of confidentiality, integrity, availability, authenticity and non-repudiation. "Confidentiality" parameter characterizes the ability to prevent the illegal distribution of personal information by participants in the educational process. "Integrity" parameter of educational content is associated with the impossibility of its illegitimate change, affecting the internal unity, logical connection in accordance with the requirements of the educational organization and federal standards. Accessibility to a digital

learning environment means the possibility of unhindered entry to DEE resources for all legitimate participants in the educational process. "Authenticity" parameter provides for the confirmation of identity and the obstacle to the ability of the subject to impersonate another user. Non-repudiation is considered as an important security parameter linked with preventing the possibility of refusing to create, receive or process information (Kuznetsova, Azhmukhamedov & Baeva, 2020).

II. The cluster of cognitive risks is associated with impairment or impairment of cognitive processes.

The following main types of possible cognitive risks of digitalization of the educational space were identified: 1) informational oversaturation of the cognitive sphere of students as a process of fixing redundant information at the levels of attention, memory and thinking, causing fatigue and reducing motivation for learning; 2) crucial transformation of students' consciousness as a process of changing the content and structural/functional mechanisms of the dynamics of consciousness, expressed in the development of "clip consciousness"; 3) devaluation of the possibilities of memory as a cognitive situation manifested in the domination of the short-term type of memory over the long-term one and the alienation of individual memory from social (cultural) memory, due to its depreciation and replacement by digital information resources; 4) decrease in the level of critical independent thinking as a process revealing itself in the dominance of the emotional-figurative type of perception and thinking over the verbal-logical type and the devaluation of analytical abilities (Khrapov, 2020).

III. The cluster of vital risks and threats associated with a significant increase in screen time accompanying the digital transformation of education.

The generalization of scientific sources and the results of focus groups surveys showed that the main risks were connected with emotional, mental and physical reboots. The organs of vision, the musculoskeletal system, and the nervous system are the most vulnerable in this regard. Excessive "screen time" can be a source of physical and psychological overexcitement for adolescence, as sleep disorders, emotional exhaustion, provokes increased activation of the visual centers; this also becomes the cause of the development of diseases of the spine. (Baeva, Khrapov, Azhmukhamedov, Grigoriev & Kuznetsova, 2020).

IV. The cluster of social risks.

It was found that the shift in lifestyle to a digital communication and educational environment for students can have certain risk-generating effects forming difficulties with socialization, interpersonal communication, social

skills, etc. Social risks have a delayed effect and can manifest themselves as communication further shifts to the digital environment. As noted by A. V. Grigoriev, one of the consequences of the digitalization of education which reduces the share of interpersonal communication may be "desocialization of the individual expressed to this or that extent, namely, deterioration of communication skills, mismatch of rules and behavioral habits in society, weakening of the sense of community, belonging to a larger social group" (Grigoriev, 2020, p. 415). This becomes a manifestation of social exclusion, infringing of the person's involvement in social relations expressed through language, behavioral specifics, etc., and contributes to the growth of alienation both between the teacher and the students and among the students themselves. This alienation "becomes a prerequisite for the development of other social risks of digitalization of education, namely trolling and bullying" (Grigoriev, 2020, p. 416).

V. The cluster of risks of addictions forming.

The factor of addictions forming associated with various forms of electronic culture is of particular concern in recent decades. An increase in the students' "screen time", and the transition of communication mainly to a virtual environment can contribute to the formation of new addictive disorders and forms of behavior, such as "screen addiction", dependence on social networks, a general growing dependence on gadgets and Internet communication. (Baeva, Khrapov, Azhmukhamedov, Grigoriev & Kuznetsova, 2020).

The risks of digitalization of communication and education are manifested in different ways in certain conditions (social well-being, age characteristics, psychological aspects of personality, etc.); therefore, attention to them should form a wide range of measures for social support of students. Such support received particular relevance in the crisis year of 2020, when all students found themselves in the conditions of a transition to digital learning.

PERSONAL SAFETY PRACTICES IN A DIGITAL LEARNING ENVIRONMENT

In 2020, as the issues of personal protection in the digital environment were becoming more acute, social practices related to ensuring security have intensified. The factors that increase social security in the digital environment of the education system, in our opinion, are various types of activity that contribute to:

1) respect for human rights, in this case the right to education;

2) protection of the individual in the digital environment from destructive social impact;
3) ensuring the communicative needs of the individual (want of communication, self-expression, social interaction) and the development of his abilities, skills that increase his social adaptation and socialization;
4) the settlement of relationships in the communicative and educational environment based on the principles of ethics, mutual respect and recognition of the rights of each of the parties to a dialogue or polylogue.

In 2020, during a pandemic, security issues in the digital environment came to the focus of attention of both researchers and practitioners. In different countries, educational organizations and ministries began to develop and implement certain elements of the security system associated with protecting students from different threats. Security issues were reflected in various guides and instructions on security in the cyber environment, posted on the websites of educational institutions, which were studied by us on the basis of the elements of content analysis and in-depth study of individual media cases (study of Internet portals of educational organizations in different countries). The following were used as the main categories for comparison:

1 sections on security in DEE;
2 safety instructions for students (meant for parents);
3 information about the types of threats in the digital environment (of their variants; for example, cyberbullying, as the most widespread type of personal abuse);
4 providing links to the addresses of the helpline or the hotline for assistance in a crisis situation;
5 links to documents on cybersecurity at the national or international level;
6 the existence of rules of ethics of conduct in the digital educational environment (from an external source, or developed in the organization).

In November-December 2020, we studied the Internet portals of educational institutions (ministries, universities, schools) in selected countries of Europe and Asia in order to analyze content related to ensuring security (including that from social risks) in the digital educational environment (DEE). The sites of the University of Tokyo, Kanagawa University (Japan), Seoul National University, Peking University, Shanghai Open University, East

China University, University of Edinburgh, New Zealand Ministry of Education, UK Ministry of Education, EU Ministry of Education, Russian Ministry of Education were studied, as well as those of Moscow State University named after M.V. Lomonosov, and National Research University Higher School of Economics. A number of universities did not publish any information on the prevention of threats in the digital environment in connection with the transition to digital education; some universities partially reflected the information, including guidelines on communication in the cyber environment, personal data protection, etc. In general, information on security in the cyber environment was presented in fragments, which showed that the policy of ensuring the protection of students is still largely at the stage of contemplation on and formation of, but not implementation. Universities in Japan were examined on the example of the websites of two universities. For instance, on the website of the University of Tokyo in the context of the transition to digital education in 2020, detailed "Rules for the safe communication of students and teachers"[1] were posted, as well as detailed instructions for working in a digital environment on various resources[2]. During 2020, the university worked in a remote format and monitored emerging problems, provided material support for students.

In December 2020, the Briefing "Towards an online hybrid class" was also held to analyze the achievements and shortcomings in the course of working in the online learning environment and preparing for the new year 2021. Instructions for students in the field of safe communication in the digital environment are not provided on the portal, issues of social cybersecurity threats, for example cyberbullying, are presented only in the scientific news section devoted to the study of professors of the University of Tokyo, who investigated this phenomenon in 2020 including its correlation with human emotional competencies using the quantitative analysis method (survey with a sample of 6403 respondents)[3].

In 2020, the website of the University of Kanagawa (Japan) provided detailed information on the transition to distance learning and the prevention of coronavirus infection; remote learning support sites were created with two versions: "For students" and "For teachers"[4]. The president of the university has allocated a one-time scholarship of 50,000 yen for students and for

1 How to let your students know your online class URL – Ground rules to safely meet instructors and students https://utelecon.github.io/en/faculty_members/let_students_know_your_url#how-to-let-your-students-know-your-online-class-url--ground-rules-to-safely-meet-instructors-and-students

2 Responses to cyberbullying Bullied victims' experiences differ by their ability to handle their own emotions. URL: https://www.u-tokyo.ac.jp/focus/en/press/z0508_00 120.html

3 Responses to cyberbullying Bullied victims' experiences differ by their ability to handle their own emotions. URL: https://www.u-tokyo.ac.jp/focus/en/press/z0508_00 120.html

4 Site of Kanagawa University. Establishment of Remote Class Support Site (24.04.2020) URL: https://www.kanagawa-u.ac.jp/english/news/details_20 151.html

the organization of their online education in 2020[1]. At the same time, issues of cybersecurity and cybersecurity were not reflected separately on the site.

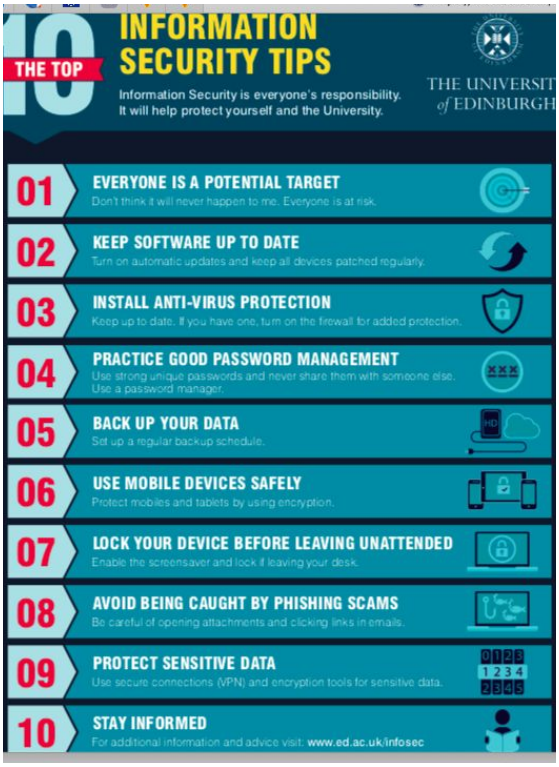

Figure 1. Website of the University of Edinburgh. Top 10 rules for information security

The analysis of the websites of universities in China was carried out on the example of Peking University and a number of universities in Shanghai. Peking University least reflected information related to the safety and protection of students in the digital environment. Only studies by university scientists involved in cybersecurity and cyber defense are noted here. At the same time, the contribution of a number of Shanghai universities to the development of measures for social and psychological support of students and parents during the period of the forced transition to distance learning should be especially noted. For example, East China Pedagogical University has developed a "Guide to Mental Health Education for Elementary and Secondary Schools" to help educators in schools during a pandemic. Shanghai University of Science and Technology subsidized mobile traffic for students, and increased the number of sign language interpreters for teaching hearing-impaired students to raise the share of online text communication in teaching. Shanghai universities launched programs for the population called

1 https://www.kanagawa-u.ac.jp/english/news/details_20160.html

"The Wisdom of Family Education" and the "Grow Up Together – Parent and Children Amusement Park" program for social adaptation in home schooling conditions, for teaching preschool parents to go in for sports with children, exercises and play useful games in conditions of lockdown[1].

Among European universities, the University of Edinburgh (UK) stands out as the best practice in social security in the digital environment. The most complete information on ensuring personal safety in the context of the transition to digital learning was presented on its website[2]. The university's website presents the basic rules for information security of students, including recommendations for data protection, for ensuring "digital well-being", for the prevention of stress, addictions, emotional and psychological disorders. The information was presented in a structured manner, in separate categories. Among the recommendations in the field of information security were such as: regular checking of privacy settings; control of tracking geolocation. In the area of social well-being, there were such recommendations: set your boundaries on the Internet (since "the constant bombardment of news reports and posts on social networks can negatively affect your mental health"); take breaks from sessions if you feel moodiness; participate in activities on the Internet to support each other. In the field of protection against negative information impact, there were such recommendations: report if you witnessed cyberbullying on the Internet. The addresses of the trust services were given. In the University of Edinburgh several resources to support students' well-being has been created, such as the Big White Wall, the Feeling Good app, and the Silver Cloud Self-Help Center.

Of Russian universities, we studied the official sites of the Moscow State University named after Lomonosov, and the Higher School of Economics, which is positioned as one of the leaders in the digitalization of education.

A page "Distance education at Moscow State University" was created on the website of the Moscow State University named after M. V. Lomonosov, which contains instructions ("7 steps") for teachers on organizing online education[3], as well as recommendations for the students to adapt to a new format of education during a pandemic.

The section "FAQ on remote work at Moscow State University" provides useful information for students on the organization of educational and extracurricular life in the context of distance education, including information on the possibility of visiting virtual exhibitions (links to the pages of the best

1 Online and Open Education in Shanghai: Emergency Response and Innovative Practice during COVID-19 Pandemic. https://iite.unesco.org/wp-content/uploads/2020/06/Online-and-Open-Education-in-Shanghai-Emergency-Response-and-Innovative-Practice-during-COVID–19-Pandemic.pdf

2 The site of University of Edinburgh. Information Security is everyone's responsibility. It will help protect yourself and the University. URL: https://www.ed.ac.uk/information-services/help-consultancy/is-skills/digital-safety-and-citizenship/staying-safe-learning-teaching-online

3 https://covid.msu.ru/

museums in the world), web travel (in Antarctica, to the International Space Station, etc.), reading online, learning foreign languages, watching films[1] in order to relieve psychological tension, and alienation from the usual environment of communication. Information on security in a digital learning environment, prevention of cybersecurity threats, their variants and personal protection was not presented on the university website; neither ethical rules for working in an online learning environment.

On the website of another leading Russian university, the National Research University Higher School of Economics, a separate page was created in 2020 with recommendations for the transition of education to a digital environment during a pandemic, which contains instructions for teachers and students. They gave recommendations on organizing classes and communicating with students in various formats[2], including a step-by-step "Memo on how to transfer classes to online type"[3]. Among the recommendations, one should especially highlight those that contain advice "How to do" and "How not to do" for the effective organization of online learning. As a reduction in the risks of a cognitive nature, we noted recommendations aimed at maintaining students' motivation to learn, as well as reducing the unnecessary burden on the student to maintain the quality of education.

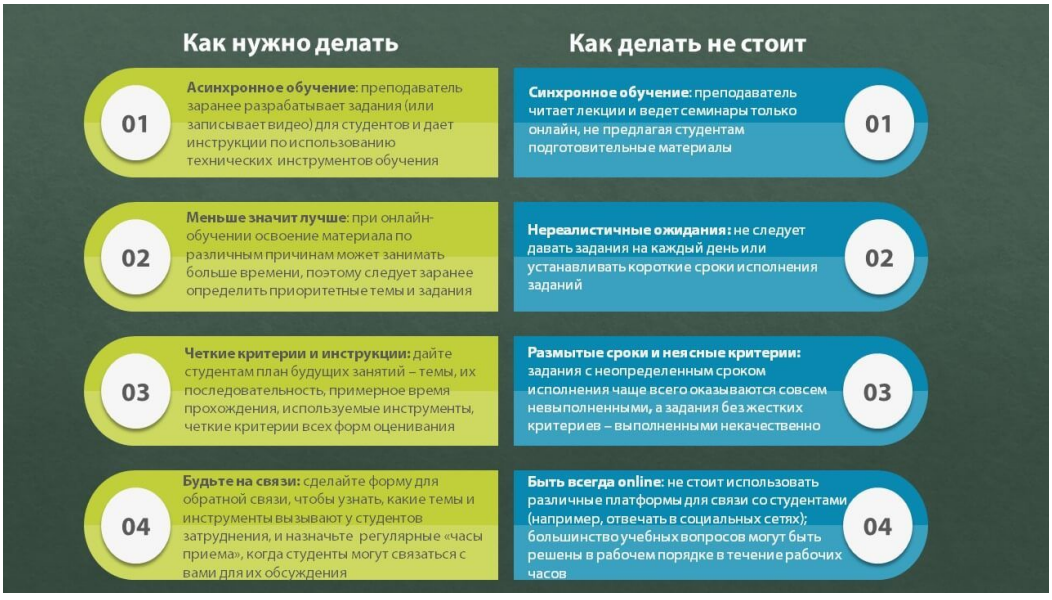

Figure 2. Site of the National Research University Higher School of Economics. Instructor Memo[3]

1 Moscow State University. Official site. 'FAQ on remote operation at Moscow State University' https://vk.com/@studsovetmsu-chem-zanyatsya

2 National Research University Higher School of Economics. Official site. Distance learning tools. URL: https://elearning.hse.ru/if_you_want_to_create

3 National Research University Higher School of Economics. Official site. Memo for the teacher: Transfer of the discipline to the online format. URL: https://elearning.hse.ru/how_to_prepare

3 Ibid. Do's and Don'ts. English version: https://elearning.hse.ru/en/how_to_prepare/

At the same time, among the instructions for teachers and students present on the site there is no prophylaxis of cybersecurity measures, protection of individual rights and dignity, countering cyber fraud, caring for manifestations of addictions and psychological disorders. Information for students is mainly containing advice on preparing for exams, for preparing for classes. National Research University Higher School of Economics, on the wide transition of its services to online learning, has developed the widest range of measures for organizing online learning, primarily from an organizational and technical position; however, as for social support measures and personal safety issues, they have not yet been given significant importance.

Analyzing these sample examples, we can draw the following conclusions. During the period of digital transition, the websites of leading universities to a greater or lesser extent provided information related to ensuring personal safety in the digital learning environment. The main focus was made on ensuring the continuity of education and instructions for teachers and students for the learning process itself. Much attention is paid to the organizational, methodical, technological aspects of working in an online learning environment. A number of universities paid special attention to cybersecurity threats and their prevention (University of Tokyo, University of Edinburgh). At the universities of Tokyo, Shanghai and Moscow State University named after Lomonosov, considerable attention was paid to measures of a socio-psychological orientation, to create a positive background, to maintain an atmosphere of solidarity in conditions of disunity and forced remoteness of students from each other and the campus.

The control over the activities of schools that are less autonomous in comparison with universities is carried out by the national ministries of education, whose websites we also studied for coverage of recommendations on ensuring social security in the cyber environment for schoolchildren.

One of the successful cybersecurity reporting cases is the New Zealand Ministry of Education website. Here, the first materials on safe behavior and learning date back to even 2015. Materials for the work of teachers with different age categories were posted on the website of the Ministry: up to 6 years old, from 5 to 16, and 16+. The website also contains a detailed guide "Digital Technologies: Safe and Responsible Use in Schools" (2015)[1]. The Guide includes descriptions of the digital technologies themselves, of the accepted forms of behavior, as well as a description of the risks and negative scenarios that are most common (cyberbullying, publishing intimate photos, organizing a fight online, recording an incident in the classroom and

1 Site of Ministry of Education of New Zealand. Digital technologies: Safe and responsible use in schools. URL: https://www.education.govt.nz/school/digital-technology/digital-technology-guide-for-schools/digital-technology-safe-and-responsible-use-in-schools/.

publishing it, etc.). Separate sections are devoted to such categories as: "Safe and responsible use of digital technologies for learning"; "Incident response", "Legislation and Incident Management"; "Responsibility and Authority of Schools"; "Using social networks and other online services in teaching and learning".The Ministry's website pays attention to the ethical principles of behavior in the conditions of online learning; it provides recommendations for regulating these issues.

Special sections on the website of the Ministry of Education of New Zealand were devoted to an overview of measures preventing and responding the incidents in DEE, the study of negative scenarios and measures to prevent them (through a system of questions and answers) (the main scenarios were the distribution of intimate photos and pornography on the network, the use of instant messages for organizing a fight, video recording of the attack). The site contains a list of criminal offenses in the digital environment (cyber-bullying, harassment and threatening behavior), links to legislation and a list of necessary literature. The section on terminology includes such concepts as "Cybersafety: Involves conduct or behavioural concerns" and "Cybersecurity: Involves unauthorized access or attacks on a computer system", where the first has a more socio-psychological and the second – technological emphasis.

In 2020, during the pandemic, a section on Covid-19 appeared on the website of the Ministry of Education of New Zealand, where detailed information about learning from home was posted, including a separate website for parents, including instructions for organizing education for children of various categories (up to children of migrants and refugees)[1]. The information was presented in 15 languages.

For certain categories (Mauri peoples), the lessons were televised. All schools were sent packages of documents and teaching materials on 50 basic disciplines (including printed ones if the children did not have access to the Internet). Specific links have been created for early childhood education counseling, counseling for schools, and for health care providers related to the pandemic.

Conclusions for the 1st case:

1) In New Zealand, in 2015, the creation of conditions for online learning in schools began.
2) An information and legal base for DEE was created at the national level.

1 Ministry of Education of New Zealand. Covid-19: Distance learning. URL: https://www.education.govt.nz/covid-19/distance-learning/

3) Guidelines have been developed for various levels of education for working in DEE.

4) During the pandemic, resources were created with educational materials, guidelines and forms for consultation and feedback not only in the state language (English), but also in the languages of the peoples living in the country or the languages of migrants.

5) Personal safety issues were fully reflected on the website of the Ministry of Education, including a detailed list of threats (their conceptual analysis), their examples, and preventive measures for different age groups of students.

This case shows an example of an effective organization of theoretical and practical work in the field of risk and threat mitigation in the digital environment.

The second case is dedicated to the website of the UK Department of Education. Information on student safety in the digital environment has been presented here since 2019. The Department's website has a comprehensive Guide to Online Safety in UK Schools that can be used by educators and parents and guardians alike. This guide describes how schools can ensure their students understanding of how to stay safe and how to behave within the future and existing curriculum requirements. One of the most important measures taken by the UK Department of Education was the decision to include from September 1, 2020, the course "Teaching Online Security" as a mandatory course in the school curriculum. Also, certain issues related to safety, on the recommendation of the Ministry, were to be included in the already existing disciplines. For example, the course "Civic Education" should now cover issues of media literacy in order to develop the ability to distinguish facts from opinions, analyze issues of freedom of speech, the role and responsibility of the media in informing and shaping public opinion.

Particular attention on the website of the UK Ministry of Education is paid to cybersecurity; the page "Online Security" provides detailed information on how to avoid online fraud (fishing), online crimes associated with extremism, violence or discrimination on various grounds. During the pandemic in 2020, the Ministry's website added columns related to the protection of teachers and students, pages for parents and guardians to ensure online safety of children, to prevent negative impact on the Internet, to set up parental controls on various devices, advice to parents and guardians to protect children from online radicalization[1]. At the request of "cyberbullying",

1 Safeguarding and remote education during coronavirus (COVID-19) (April 2020). URL: https://www.gov-.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19#safeguarding-pupils-and-teachers-online

63 results have been generated on the Ministry's website (2018-2020) on the measures providing assistance, study and prevention of this social phenomenon (01/04/2021). This topic is one of the most important in the field of studying social threats and protection for the young people in the Internet, and it rightly attracts the attention of educators and specialists. An important role was given on the Ministry's website to providing psychological support to students, helping students to protect themselves from stress in the context of digital education.[1] "Public Health England Parent and Guardian Guidelines" are developed to help organize student routines that will help children feel safe in the face of uncertainty.[2]

Conclusions for the 2nd case:

1) Online safety issues were highlighted as priorities for study in the school curriculum;
2) Safety guidelines for parents and guardians in the digital environment include aspects of countering the spread of violence, extremism, discrimination;
3) During the pandemic, resources have been created to protect both students and teachers;
4) A system of measures has been developed to support parents, as well as to train them to monitor children and help them with safety issues;
5) Special attention was paid to the problems of the emotional and psychological state of students and protection from stress;
6) The types of threats in the digital environment are presented differentially, and special attention is paid to the most socially dangerous and widespread destructive informational influences.

The third case is devoted to the website of the Ministry of Education of the Russian Federation.

Since March 2020, hotlines have been created and operated on the website of the Ministry for methodological support for teachers, parents, school principals, students of secondary vocational education, as well as people with disabilities. A specialized section has been created on the Ministry's website to help organize home education using distance technologies, containing instructions and methodological materials for teachers

1 Safeguarding and remote education during coronavirus covid-19/ URL: https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19#providing-pastoral-care-remotely

2 URL: // https: www.gov.uk/government/publications/covid-19-guidance-on-supporting-children-and-young-peoples-mental-health--during-the-coronavirus-covid-19-outbreak#helping-children-and-young-people-cope-with-stress

and schools. As material and social support, 500 thousand children and 23 thousand teachers received computers and Internet access free of charge.[1] On Children's Day, June 1, 2020, an open lesson "Cybersecurity and rules of conduct on the Internet" was held to develop information security skills in schoolchildren.[2] At the same time, there are no separate sections dedicated to recommendations in the field of security and protection in the digital environment on the site, as well as ethical codes for work and study. For the query "cyberbullying", the Ministry of Education website did not provide any results. The data obtained indicate that security issues in the digital environment are still largely underestimated and require a comprehensive study to be updated.

Conclusions for the 3rd case:

1) Methodological materials for organizing online education in the pandemic were posted on the website of the Ministry of Education of the Russian Federation.
2) Measures were taken to provide material support to citizens to solve the problem of access to educational resources.
3) The problem of security in the digital learning environment did not receive documentary support and recommendations for teachers and students.

The fourth media case was devoted to the analysis of the website of the European Commission on the regulation of online education. Strategically important steps for the EU countries on security issues in the field of digital education were developed at the 3rd European Education Summit (12.12.2020). Here, the development of digital competencies and increasing information literacy of the population, as well as bridging the digital divide were named the main tasks.[3] At the summit, the "Digital Education Action Plan (2021-2027)" was adopted, in which the problems of digital education that arose in 2020 were also noted. First of all, they included the lack of equal access for all students to Internet resources and technical un-readiness for distance learning. Based on the monitoring carried out before the summit, it was revealed that the most vulnerable were junior and middle schoolchildren, who themselves could not organize their own learning process. In families

1 URL: https://edu.gov.ru/press/3079/opyt-rossii-po-organizacii-bezopasnogo-uchebnogo-processa-vysoko-ocenili-v-sovete-evropy
2 https://edu.gov.ru/press/2541/minprosvescheniya-rossii-udelyaet-osoboe-vnimanie-bezopasnosti-obrazovatelnogo-kontenta-v-period-distancionnogo-obucheniya
3 Digital Education Action Plan (2021-2027) URL: https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en

with higher educated parents, the transition to digital leaning was more successful, and the children received the necessary assistance. Such problems of digital learning as high overload of information and tasks for students, introduction of false information and extraneous content, insecurity of personal data were noted.[4] To address emerging and potential threats, the European Commission's Plan provides for the development of common guidelines for teachers and teaching staff on increasing digital literacy and combating disinformation through education and training.[5] Thus, the importance of preventive actions in the field of protection against falsification of information, fakes, violation of the integrity of educational content or the use of low-quality material for educational activities is noted.

Another no less important area of the Action Plan implementation is the development of ethical standards for the use of artificial intelligence in education, which is also an important measure for the prevention of possible social and legal risks in the relationship "person – AI", in which incorrect actions that harm a person and his dignity are possible. At the same time, the issues of the security of the digital learning environment in social, psychological, vital, addictive relations have not yet been reflected in the Digital Education Action Plan. However, it should be noted that cyberbullying issues in Europe have attracted more and more attention among scientists and practitioners in recent years.

This case shows that in the Digital Education Action Plan for the EU countries:

1) The issues of personal safety in the digital environment are considered as priorities, along with the issues of organizing and expanding digital learning, overcoming the digital divide, etc.;
2) Specialized sections on protecting a person from threats are not presented in the document;
3) Issues of cyber ethics, including ethics of human relations with AI in the educational environment, are being raised as topical in the coming years;
4) The work of the European Commission pays great attention to countering social threats in the cyber environment (cyberbullying, etc.), which are considered in a set of measures to protect human rights and dignity.

4 Digital Education Action Plan (2021-2027) URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1602778451601&uri=CELEX%3A52020DC0624

5 Digital Education Action Plan (2021-2027) URL: https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en

CONCLUSION

Thus, the following conclusions can be drawn regarding the assessment of security issues in a digital learning environment and their coverage in educational practices:

1. In the context of digital transformation, the learning system significantly changes the nature of the social interaction of its subjects, breaking old ties and forming new ones. The role of social skills, and interpersonal communication, formed in the process of educational and extracurricular activities, is extremely important for the formation of personality, and they should also be given an important place in the context of digital transformation. A significant role in the digital transformation is played by the social well-being of the student, digital hygiene and the guarantee of the protection of his rights and freedoms in the digital environment. Interpersonal communication among students in virtual classrooms is being replaced by communication in social networks, which changes its nature and forms new social phenomena (including risk-generating ones associated with destructive information impact). In these conditions, prophylaxis of the social security in the digital educational environment is becoming one of its important components in this system, which ensures the protection of the rights and freedoms of the individual.

2. The guarantee of social protection of individual rights in the information society should be associated first of all with the possibility of choosing a form of education (traditional, distance or hybrid), which should be taken into account when forming strategic documents in the field of education development at the national and regional levels. Students and parents should have the right to decide whether it is worth turning to distance learning in a digital environment, unless it is caused by *force majeure*.

Another important parameter of social guarantees of human rights to education in the digital environment is the availability of resources, the provision of which should not be completely transferred to the families of students.

3. The digital learning environment, created by order of modern governments in various countries, is becoming a concentration of large volumes of educational materials, tests and assignments performed by students in many ways autonomously, the verification of which will be supplemented in the near future with specialized artificial intelligence. This will create conditions under which the social background that motivates learning and activity, the formation of moral experience, the dialogue with the Other, including the experience of communication in the intercultural sphere, is practically absent and is replaced by the cyber environment, simulative community and communication. This requires the development of a system of social support

and accompanying students, designed to strengthen social and emotional skills, moral forms of behavior in the digital environment.

The tasks of the social support system should include, among other things:

1) supporting families with technology difficulties and creating equal educational opportunities;
2) support of interpersonal communication and the formation of social skills of the individual;
3) support of a positive social and emotional state in virtual classrooms;
4) prevention of deviant manifestations and social threats in the network interaction of students, including cyberbullying;
5) development of codes of ethics for online education and training courses on the basics of safe behavior in the cyber environment.

4. Social security and well-being depend on the prevention of threats in the cyber environment that can intentionally harm the individual. Websites of educational organizations post materials on the prevention and countermeasures of personal threats in the digital environment. However, an understanding of the relevance of these steps in a broad sense has not yet been achieved; a lag in responding to such challenges can lead to tragic consequences. Informing about existing threats alone is not sufficient to counter them; a system of measures in educational institutions is needed to counter cybersecurity threats of a socio-psychological orientation (along with the protection of information and personal data).

5. In the education system in various countries, security issues in the digital learning environment remain largely underestimated. A number of universities in Asia and Europe demonstrate a high degree of concern for cybersecurity, while in Russian universities these problems remain on the periphery of attention. It should be noted that European universities and ministries of education are more focused not on protecting the system from cybersecurity threats, but on protecting human rights and dignity. In Russia, using the example of Moscow State University, one can note that high attention is paid to social and psychological support of students in the digital environment as a prevention of network social threats.

6. The study of the best practices in the field of personal protection from social cybersecurity threats becomes, in the context of digitalization of education, an opportunity to increase the competencies of each educational institution at all levels of education. In this regard, it is effective to create a databank at the international level, accumulating measures to prevent threats, develop

ethical codes of communication in the digital environment, including relations between humans and artificial intelligence.

The system of social support for students as one of the important elements of the digital learning environment should become one of the sources of prevention of possible deviations, addictions, destructive or self-destructive behavior, as well as the basis for protecting the individual from threats in the cyber environment, violation of the rights and freedoms and dignity of the individual, protection of personal data , to maintain and develop the social environment of communication, to strengthen the skills of socialization of the individual both in the conditions of electronic culture and in real communication.

ACKNOWLEDGMENTS

The article was prepared in terms of the research project "Assessment of the impact of digitalization of educational and social space on a person and the development of a safe communication and educational environment", Russian Foundation for Basic Research (RFBR) grant № 19-29-14 007 МК.

References

A3, E. (2018, September 14). Digital Education Action Plan (2021-2027) [Text]. Retrieved from Education and Training—European Commission website: https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en

Alghamdi, Y. (2016). *Negative Effects of Technology on Children of Today*. Oakland: Oakland University. doi: 10.13140/RG.2.2.35724.62089

Baeva, I. A. (2002). *Mental safety in education*. St. Petersburg: Publishing house "Soyuz". (In Russian).

Baeva, L. (2014). E-Culture. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology: In 10 vol.: Vol. IX* (3rd ed., pp. 6847–6854). USA: IGI-Global.

Baeva, L. V. (2013). E-culture: Experience of philosophical analysis. *Voprosy Filosofii*, (5), 75–83. (In Russian).

Baeva, L. V., Khrapov, S. A., Azhmukhamedov, I. M., Grigoriev, A. V., & Kuznetsova, V. Yu. (2020). The Digital Curve in Russian Education: From Problems to Opportunities. *Values and meanings*, (5), 28–44. doi: 10.24411/2071-6427-2020-10 043 (In Russian).

Chu, H.-C. (2014). Potential Negative Effects of Mobile Learning on Students' Learning Achievement and Cognitive Load—A Format Assessment Perspective. *Journal of Educational Technology & Society*, *17*(1), 332–344.

Cybersecurity and Rules of Conduct on the Internet. (2020). Retrieved from Ministry of Education of the Russian Federation website: https://edu.gov.ru/press/2541/minprosvescheniya-rossii-udelyaet-osoboe-vnimanie-bezopasnosti-obrazovatelnogo-kontenta-v-period-distancionnogo-obucheniya (In Russian).

Education in New Zealand. (2020, December 7). Retrieved from Home learning website: https://www.education.govt.nz/covid-19/distance-learning/

Establishment of Remote Class Support Site. (2020, April 24). Retrieved from Site of Kanagawa University website: https://www.kanagawa-u.ac.jp/english/news/details_20 151.html

Fundação Telefônica Vivo. (2016). *Assessment experiences in digital technologies in education.* São Paulo. Retrieved from https://unesdoc.unesco.org/ark:/48 223/pf0 000 247 330

Gable, G., Sedera, D., & Chan, T. (2008). Re-conceptualizing Information System Success: The IS-Impact Measurement Model. *Journal of the Association for Information Systems*, *9*(7). doi: 10.17705/1jais.00164

How to let your students know your online class URL – Ground rules to safely meet instructors and students. (n.d.). Retrieved from Utelecon website: https://utelecon.adm.u-tokyo.ac.jp/faculty_members/old/let_students_know_your_url.html

How to prepare for the transition to a distance learning format. (2020). Retrieved from https://elearning.hse.ru/how_to_prepare (In Russian).

Iljuschenko, N. S. (2019). Digital learning: Perspectives and Risks of the Digital Curve in Education. *Designing the Future. Problems of Digital Reality: Proceedings of the 2nd International Conference (February 7-8, 2019, Moscow)*, 215–225. Moscow: M.V. Keldysh Institute for Applied Mechanics. Retrieved from https://keldysh.ru/future/2019/20.pdf doi:10.20948/future-2019-20 (In Russian).

Information Security is everyone's responsibility. It will help protect yourself and the University. (2021). Retrieved from The site of University of Edinburgh website: https://www.ed.ac.uk/information-services/help-consultancy/is-skills/digital-safety-and-citizenship/staying-safe-learning-teaching-online

Johnston, J., & Barker, L. T. (2002). *Assessing the impact of technology in teaching and learning: A sourcebook for evaluators.* Ann Arbor, MI: Institute for Social Research, University of Michigan.

Karpova, D. N. (2016). *The Risks of Continuous Online Communication: Theoretical and Methodological Approaches to the Study* (PhD Thesis). MGIMO, Moscow. (In Russian).

Khrapov, S. A. (2020). Risks of Forming a "Technogenic (Digital) Identity" in the Digitalization of Educational Space. *Vestnik of Tver State University. Series: Philosophy.*, (2), 7–13. (In Russian).

Kuznetsova, V. Y., Azhmukhamedov, I. M., & Baeva, L. V. (2020, May 13). *Analysis of Information Risks and Strategies for Protecting Schoolchildren from the Negative Consequences of Digitalization of Education.* 244–249. Atlantis Press. doi: 10.2991/assehr.k.200509.045

Leaflet for students on information security of children. (2020). Retrieved from http://sites.petersburgedu.ru/media/32/docs/3461/addition MZQQlFX.pdf (In Russian).

MSU. Official website. "FAQ on Remote Mode of Work at MSU". (n. d.). Retrieved from https://vk.com/@studsovetmsu-chem-zanyatsya (In Russian).

Mustafaoğlu, R., Zirek, E., Yasacı, Z., & Razak Özdinçler, A. (2018). The Negative Effects of Digital Technology Usage on Children's Development and Health. *Addicta: The Turkish Journal on Addictions*, *5*(2). doi: 10.15805/addicta.2018.5.2.0051

Online and Open Education in Shanghai: Emergency Response and Innovative Practice during COVID-19 Pandemic. (2020). Retrieved from UNESCO IITE website: https://iite.unesco.org/publications/online-and-open-education-in-shanghai-emergency-response-and-innovative-practice-during-covid-19-pandemic/

Panchenko, O., Mukhametzyanova, F., & Khayrutdinov, R. R. (2019). Challenges and risks to personal safety in the digitalization of education. In D. V. Sochivko (Ed.), *Psychology of the XXI Century: Challenges, Search, Vectors of Development. Proceedings of the All-Russian Symposium of Psychologists.* (pp. 640–645). Ryazan: Academy of the Russian Federal Penitentiary Service. (In Russian).

Responses to cyberbullying: Bullied victims' experiences differ by their ability to handle their own emotions. (2020, June 29). Retrieved from ScienceDaily website: https://www.sciencedaily.com/releases/2020/06/200 629 120 145.htm

Russia's experience in organizing a safe learning process. (2020). Retrieved from https://edu.gov.ru/press/3079/opyt-rossii-po-organizacii-bezopasnogo-uchebnogo-processa-vysoko-ocenili-v-sovete-evropy (In Russian).

Safeguarding and remote education during coronavirus COVID-19. (2020). Retrieved from GOV.UK website: https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

Safety of the digital environment in a distance learning environment for children under 18. (n. d.). Retrieved from http://sites.petersburgedu.ru/media/32/docs/3463/additions/8B.pdf (In Russian).

Schneider, L. B., & Symanyuk, V. V. (2017). The User in the Information Environment: Digital Identity Today. *Psychological Research*, *10*(52), 7. (In Russian).

Semenov, A. L. (2019). Goals of General Education in a Digital World. Informatization of Education and Methodology of E-learning : Proceedings of the III International Scientific Conference Krasnoyarsk, September 24-27, 2019., 383–388. Krasnoyarsk: Siberian Federal University. (In Russian).

Strekalova, N. (2019). Risks of implementing digital technologies in education. *Bulletin of Samara University. History. Pedagogy. Philology*, *25*(2), 84. doi: 10.18287/2542-0445-2019-25-2-84-88 (In Russian).

Taleb, N. (2015). *Black Swan. Under the sign of unpredictability*. Moscow: KoLibri.. (In Russian).

Tawafak, R. M., Romli, A. B., Arshah, R. bin A., & Almaroof, R. A. S. (2018). Assessing the Impact of Technology Learning and Assessment Method on Academic Performance: Review Paper. *Eurasia Journal of Mathematics, Science and Technology Education*, *14*(6). doi: 10.29333/ejmste/87 117

Список литературы

A3, E. (2018, September 14). Digital Education Action Plan (2021-2027) [Text]. Retrieved from Education and Training—European Commission website: https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en

Alghamdi, Y. (2016). *Negative Effects of Technology on Children of Today*. Oakland: Oakland University. doi: 10.13140/RG.2.2.35724.62089

Baeva, L. (2014). E-Culture. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology: In 10 vol.*: *Vol. IX* (3rd ed., pp. 6847–6854). USA: IGI-Global.

Chu, H.-C. (2014). Potential Negative Effects of Mobile Learning on Students' Learning Achievement and Cognitive Load—A Format Assessment Perspective. *Journal of Educational Technology & Society*, *17*(1), 332–344.

Education in New Zealand. (2020, December 7). Retrieved from Home learning website: https://www.education.govt.nz/covid-19/distance-learning/

Establishment of Remote Class Support Site. (2020, April 24). Retrieved from Site of Kanagawa University website: https://www.kanagawa-u.ac.jp/english/news/details_20 151.html

Fundação Telefônica Vivo. (2016). *Assessment experiences in digital technologies in education.* São Paulo. Retrieved from https://unesdoc.unesco.org/ark:/48 223/pf0 000 247 330

Gable, G., Sedera, D., & Chan, T. (2008). Re-conceptualizing Information System Success: The IS-Impact Measurement Model. *Journal of the Association for Information Systems*, *9*(7). doi: 10.17705/1jais.00164

How to let your students know your online class URL – Ground rules to safely meet instructors and students. (n.d.). Retrieved from Utelecon website: https://utelecon.adm.u-tokyo.ac.jp/faculty_members/old/let_students_know_your_url.html

Information Security is everyone's responsibility. It will help protect yourself and the University. (2021). Retrieved from The site of University of Edinburgh website: https://www.ed.ac.uk/information-services/help-consultancy/is-skills/digital-safety-and-citizenship/staying-safe-learning-teaching-online

Johnston, J., & Barker, L. T. (2002). *Assessing the impact of technology in teaching and learning: A sourcebook for evaluators.* Ann Arbor, MI: Institute for Social Research, University of Michigan.

Kuznetsova, V. Y., Azhmukhamedov, I. M., & Baeva, L. V. (2020, May 13). *Analysis of Information Risks and Strategies for Protecting Schoolchildren from the Negative Consequences of Digitalization of Education.* 244–249. Atlantis Press. doi: 10.2991/assehr.k.200509.045

Mustafaoğlu, R., Zirek, E., Yasacı, Z., & Razak Özdinçler, A. (2018). The Negative Effects of Digital Technology Usage on Children's Development and Health. *Addicta: The Turkish Journal on Addictions*, *5*(2). doi: 10.15805/addicta.2018.5.2.0051

Online and Open Education in Shanghai: Emergency Response and Innovative Practice during COVID-19 Pandemic. (2020). Retrieved from UNESCO IITE website: https://iite.unesco.org/publications/online-and-open-education-in-shanghai-emergency-response-and-innovative-practice-during-covid-19-pandemic/

Responses to cyberbullying: Bullied victims' experiences differ by their ability to handle their own emotions. (2020, June 29). Retrieved from ScienceDaily website: https://www.sciencedaily.com/releases/2020/06/200 629 120 145.htm

Safeguarding and remote education during coronavirus COVID-19. (2020). Retrieved from GOV.UK website: https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

Tawafak, R. M., Romli, A. B., Arshah, R. bin A., & Almaroof, R. A. S. (2018). Assessing the Impact of Technology Learning and Assessment Method on Academic Performance: Review Paper. *Eurasia Journal of Mathematics, Science and Technology Education*, *14*(6). doi: 10.29333/ejmste/87 117

Баева, И. А. (2002). *Психологическая безопасность в образовании.* Санкт-Петербург: Издательство «СОЮЗ».

Баева, Л. В. (2013). Электронная культура: Опыт философского анализа. *Вопросы Философии*, (5), 75–83.

Баева, Л. В., Храпов, С. А., Ажмухамедов, И. М., Григорьев, А. В., & Кузнецова, В. Ю. (2020). Цифровой поворот в российском образовании: От проблем к возможностям. *Ценности и смыслы*, (5), 28–44. doi: 10.24411/2071-6427-2020-10 043

Безопасность цифровой среды в условиях дистанционного обучения детей до 18 лет. (б. д.). Извлечено от http://sites.petersburgedu.ru/media/32/docs/3463/additions/8B.pdf

Ильюшенко, Н. С. (2019). Digital learning: Перспективы и риски цифрового поворота в образовании. *Проектирование Будущего. Проблемы Цифровой Реальности: Труды 2-й Международной Конференции (7-8 Февраля 2019 г., Москва)*, 215–225. Москва: ИПМ им. М.В.Келдыша. Retrieved from https://keldysh.ru/future/2019/20.pdf doi:10.20948/future-2019-20

Как подготовиться к переводу обучения на дистанционный формат. (2020). Извлечено от https://elearning.hse.ru/how_to_prepare

Карпова, Д. Н. (2016). *Риски непрерывной онлайн-коммуникации: Теоретико-методологические подходы к изучению* (Диссертация кандидата социологических наук). МГИМО, Москва.

Кибербезопасность и правила поведения в сети Интернет. (2020). Извлечено от Министерство просвещения Российской Федерации website: https://edu.gov.ru/press/2541/minprosvescheniya-rossii-udelyaet-osoboe-vnimanie-bezopasnosti-obrazovatelnogo-kontenta-v-period-distancionnogo-obucheniya

МГУ. Официальный сайт. «FAQ по дистанционному режиму работы в МГУ». (б. д.). Извлечено от https://vk.com/@studsovetmsu-chem-zanyatsya

Опыт России по организации безопасного учебного процесса. (2020). Извлечено от https://edu.gov.ru/press/3079/opyt-rossii-po-organizacii-bezopasnogo-uchebnogo-processa-vysoko-ocenili-v-sovete-evropy

Памятка для обучающихся об информационной безопасности детей. (2020). Извлечено от http://sites.petersburgedu.ru/media/32/docs/3461/addition MZQQlFX.pdf

Панченко, О., Мухаметзянова, Ф., & Хайрутдинов, Р. Р. (2019). Вызовы и риски личной безопасности в условиях цифровизации образования. В Д. В. Сочивко (Ред.), *Психология XXI века: Вызовы, поиск, векторы развития. Сборник материалов Всероссийского симпозиума психологов* (сс. 640–645). Рязань: Академия ФСИН России.

Семенов, А. Л. (2019). Цели общего образования в цифровом мире. *Информатизация образования и методика электронного обучения : материалы III Междунар.*

науч. конф. Красноярск, 24–27 сентября 2019 г., 383–388. Красноярск: Сибирский федеральный университет.

Стрекалова, Н. (2019). Риски внедрения цифровых технологий в образование. *Вестник Самарского университета. История. Педагогика. Филология*, *25*(2), 84. doi: 10.18287/2542-0445-2019-25-2-84-88

Талеб, Н. (2015). *Черный лебедь. Под знаком непредсказуемости.* Москва: КоЛибри.

Храпов, С. А. (2020). Риски формирования «техногенной (цифровой) идентичности» в условиях цифровизации образовательного пространства. *Вестник Тверского государственного университета. Серия: Философия*, (2), 7–13.

Шнейдер, Л. Б., & Сыманюк, В. В. (2017). Пользователь в информационной среде: Цифровая идентичность сегодня. *Психологические Исследования*, *10*(52), 7.