Information Security Risks of Distance Learning Software in the Sphere of Education as an Element of Critical Information Infrastructure

Yuriy Sosnovskiy [a], Veronika Ilyina [a] and Victor Milyukov [a]

[a] *Institute of Physics and Technical Sciences, Crimean Federal V. Vernadsky University, 265007, Russian Federation*

Abstract

A number of software tools, that can be used in the organization of distance learning interaction via the Internet, has been studied in the paper. The tools have been analyzed against basic conditions of information security accreditation, such as a secure data transfer protocol, personal data transfer to a third party, cases of hacking, and sanctions restrictions to date.

Information security risks of a teacher's digital tools have been evaluated taking into account the broad scope of the educational process and the number of its participants. The damage from the use of such tools has been related to the one from critical information infrastructure control objects.

Keywords [1]

Information security, a teacher's digital tools, distance learning

1. Introduction

The global economy is rapidly going digital. The patterns of interaction between economic and legal entities and, which is of utmost importance, educational institutions activities that can be converted into electronic format are also undergoing digital transformations. As a result, distance learning is becoming increasingly popular. Such distance form of educational interaction is cheaper for all the parties of the educational process, and there also appear more and more teacher's digital tools (TDT) that facilitate such interaction.

2. Purpose and objectives of the research

Today, the typical forms of interaction between an educational establishment and a student in the Russian Federation imply the following:

An educational organization must have an electronic information and educational environment (EIEE). Its main objectives are set out in the Federal state educational standards, and it should provide [1]:

- free access to the curricula, work programs of the modules, internship and courses, as well as to educational publications in the electronic form and educational resources on the Internet;
- saving the student's completed assignments and the grades [1].

If a training program is implemented using e-learning or distance learning (if it is licensed), the EIE should additionally provide [1]:

SLET-2020: International Scientific Conference on Innovative Approaches to the Application of Digital Technologies in Education, November 12-13, 2020, Stavropol, Russia

EMAIL: sosnovskiy.yv@cfuv.ru (Yuriy Sosnovskiy); nika.ilyina@mail.ru (Veronika Ilyina); milyukov.vv@cfuv.ru (Victor Milyukov)
ORCID: 0000-0003-3807-5297 (Yuriy Sosnovskiy); 0000-0003-4165-5620 (Veronika Ilyina); 0000-0002-0429-8540 (Victor Milyukov)

- recording of the educational process events and keeping track of the students' progress in the course of mastering the educational curriculum;
- asynchronous and synchronous interaction between students and teachers.

Federal state standards for secondary education [2] contain more detailed requirements for the information and educational environment of the organization (IEE), which should provide:

- information and methodological support for educational activities;
- organization of various forms of individual and group activities;
- monitoring and recording the progress and results of educational activities;
- modern procedures and tools for creating, searching, collecting, analyzing, processing, storing and presenting information;
- interaction between all the participants in the distance learning process.

It should be noted that the requirement that the EIEE should ensure the interaction between the participants in the educational process is only stipulated for the educational programs that include electronic or distance learning forms of the educational process, which is not often common practice. But unfortunately, EIEE does not always have enough tools to meet all the needs of the educational process participants in terms of electronic interaction.

As practice shows, in a considerable number of cases, EIEE is implemented so as to meet the requirements of the regulatory authorities. At the same time, such limited tool set does not provide convenient instruments for communication and, as a result, progressive teachers have to look for their own methods of transmitting and distributing electronic educational materials, and to use the TDT that are more suitable for them.

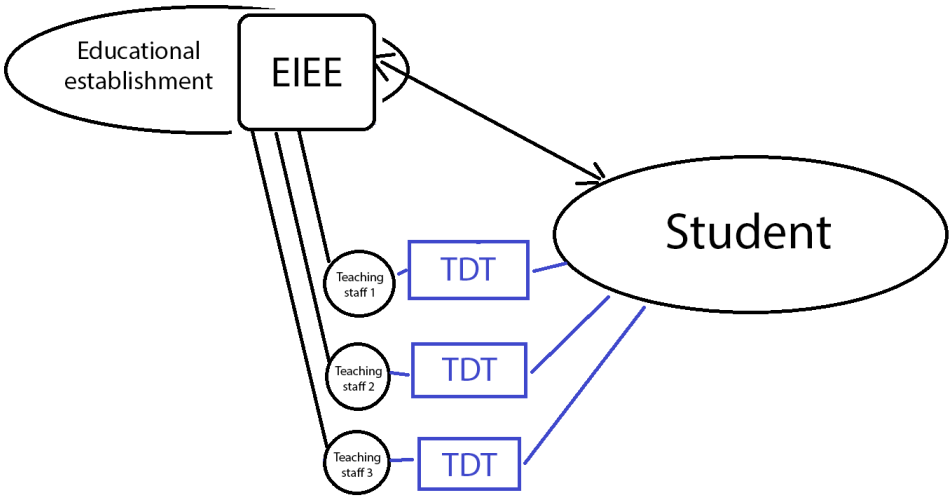

Figure 1: Typical electronic interaction between the educational establishment and the student

Thus, the importance of a teacher's digital tools, used to ensure electronic interaction between the teacher and the student, significantly increases.

3. Digital tools of the teacher. Overview and analysis

3.1. BigBlueButton webinar platform

BigBlueButton platform (BBB) is a free software system for web conferences. The major problem with the system is that the BigBlueButton client works using the browser extension for Adobe Flash, official support for which ends in 2020. Another disadvantage is relatively high pressure on the server's computational capacity. The features of the BBB system are as follows [3]:

- supports working simultaneously with a large group of students, for example, up to 100 people or more;
- provides video recording function. You can also save images and notes that were created on the electronic board during the lecture;

- the BBB platform can be integrated with Moodle due to a special module.

At the same time, the system is based on outdated technologies, and BBB does not work on Apple computers and smartphones with iOS.

3.2. Discord messenger platform

Discord is a popular application that is used primarily for voice communication. It was experimentally established that the optimal number of participants is up to 25-30 people. The maximum number allowed by the system is 50 people.

The system has some features particularly useful for the educational process:

- provides high-quality voice communication in the "General chat" mode. The minimum computer system requirements are reasonable, and there are modes both for automatically turning on the microphone and for using the dedicated button;
- allows you to arrange a streaming broadcast of the desktop screen or selected windows on your computer;
- it is possible to work both in the application and directly from the browser, which is convenient

At the same time, as the practice of using this software tool during the distance learning process has shown, it is advisable to introduce a local administrator of virtual servers and platform channels to correctly organize the interaction between the participants. The platform enables you to work effectively when active oral interaction is required both individually and in small groups – for practical work, collecting reports on laboratory work, and for lecturing in small groups.

3.3. YouTube as a platform for hosting online lectures

For a teacher YouTube has the following advantages:

- provides storage and seamless access to video contents;
- has convenient tools for analyzing users' viewing, which allows you to identify fragments of lectures or videos that arouse the greatest interest in the audience;
- video materials can be distributed among the students and also in the public domain.

3.4. Programs for remote computer management

Sometimes when working individually students can come across the problems which solutions require tutor's assistance. In this case, it is convenient to use programs that provide remote computer management. An example is the TeamViewer program.

The program provides not only computer management but also collaboration facilities. You can work collaboratively on documents online in real time, work effectively on software codes and other materials, and also – in the areas that don't have ready-made solutions.

All major operating systems are supported: Windows, MacOS, Linux, iOS, and Android. Among the features of the program, there is also holding online conferences, which though has a limit of 25 participants. At the same time, it should be noted that this program poses a potential threat to the information security of the user's computer due to the potential vulnerabilities of both the program and the need to open port 5938 for external access via TCP/UDP protocols.

3.5. Online conference programs. ZOOM

ZOOM is one of the most popular programs for online conferencing. Unlike BigBlueButton and many similar systems that use Adobe Flash technology for video transmission, ZOOM has implemented a real-time video content transmission technology — WebRTC (Web Real-Time Communication). You can set a password for the conference, invite participants by URL or email, and broadcast audio and images from your computer. There is a 40-minute limit on the length of the session for a free account.

It is also worth noting that in some regions, the use of this program without additional software is simply impossible due to various political issues and related restrictions. In addition, there is a significant number of instances when critical vulnerabilities were discovered in Zoom: for example, the MacOS user has to join a Zoom call with an activated video camera, what is more, there is no request for the authorization of switching on the camera; unauthorized connections to the broadcasts of strange people, password leaks, etc.

3.6. Programs for graphic illustrations. Online boards

In the process of distance learning, it is often essential to illustrate materials and get continuous feedbackб just as a teacher often does in a traditional classroom using a board or a smart- board. A teacher can arrange voice interaction via a convenient program, such as Discord, described above. And as to visualization, it can be effected through, for example, the AWWApp service. It does not require installation, you just need to go to the site, send your students an invitation to join the session, and work with the screen just as with a real board. In the graphics space you can make drawings, insert formulas, notes, etc. Due to the fact that the graphics space is shared, all participants can work in it at the same time. Accordingly, the teacher can give graphic tasks to the students and monitor their performance in the live mode.

The free version contains advertisements unlike the fee-based version. Also, with the paid version you can create multiple pages and upload files in .pdf format to the graphics space.

3.7. Video broadcasts in social networks

Today, the vast majority of the educational process participants have accounts on social networks. As an example, let us have a look at the Vkontakte network. It can be successfully used for distance learning under the condition that so-called "broadcasts" are arranged. The advantages of providing video content via social networks are the following:

- students just need to click on the link to the broadcast, there is no need to download any special application;
- the broadcast record is saved on the author's page and can be viewed at any convenient time;
- the record can be viewed by all those who take interest in the subject, which is both a disadvantage if you need to limit the number of viewers, and an advantage if you want to share the information with a vast number of people.

At the same time, to organize broadcasting, the teacher needs to install video recorder software and follow a certain algorithm for generating a unique broadcast key and making the broadcast itself.

3.8. Conclusions on information security of using a teacher’s digital tools

The basic criteria for evaluating the safety of using digital teacher's tools that can be useful to ordinary users are shown in table 1.

Table 1

Basic criteria of TDT information security

Teacher’s digital tool (TDT)	Secure protocol	Personal data transfer to a third party	Administration difficulty	Known instances of hacking	Restrictions due to sanctions
BugBlueButton (on your own servers)	TLS	No	High	Unlikely	No

Continuation of the table 1

Basic criteria of TDT information security

Teacher's digital tool (TDT)	Secure protocol	Personal data transfer to a third party	Administration difficulty	Known instances of hacking	Restrictions due to sanctions
Discord	end-to-end: TLS, DTLS, xsalsa20	Yes	Average	Yes	No
YouTube	Yes	Yes	Average	Leakage of users' passwords	No
TeamViewer	2048-bit keys RSA and 256-bit AES-by encrypting sessions	Yes, when registering an account	Moderate	Leakage of users' passwords, hacking through TeamViewer ID	Yes
ZOOM	TLS *	Yes, registration is required	Moderate	Multiple reports about the issues [4]	Yes
AWWApp, basic version	TLS	No	Minimum	No	No
Broadcasting in VK	TLS	Yes, registration is required**	Average	Leakage of users' passwords	No

* end-to-end encryption was declared. However, in practice, it is the usual TLS and a video stream is open to ZOOM servers

** Vkontakte is a Russian company. Website vk.com is listed in the register of information dissemination organizers under the number 4-PP, the date of its entry is September 4, 2014.

The analysis of the table shows that the majority of the TDT have an extremely high vulnerability from external cyber threats, as well as from the international restrictions policy, which also applies to the software market, including access to information resources.

Table 2

Features of storing and processing user data

Teacher's digital tools	Compliance with regulatory documents on storage and processing of personal data in information systems	Use of cryptographic information security tools (CIST) with up-to-date Federal Security Service (FSS) certificates	Location of the hosting (the Russian Federation / not the Russian Federation)
BugBlueButton (on your own servers)	Yes, no client registration is required.	Technically possible	RF (technically possible)
Discord	No, when registering a real full name	No	Not RF

Continuation of the table 2

Features of storing and processing user data

Teacher's digital tools	Compliance with regulatory documents on storage and processing of personal data in information systems	Use of cryptographic information security tools (CIST) with up-to-date Federal Security Service (FSS) certificates	Location of the hosting (the Russian Federation / not the Russian Federation)
BugBlueButton (on your own servers)	Yes, no client registration is required.	Technically possible	RF (technically possible)
Discord	No, when registering a real full name	No	Not RF
YouTube	No, when registering a real full name, because the same email address as in Google is used.	No	Not RF
TeamViewer	Does not require a full name, only a nickname and an email address.	No	Not RF
ZOOM	No registration required on the client side	No	Not RF
AWWApp basic version	No registration required for basic functionality	No	Not RF
VK broadcasts	** declared compliance with the rules 152-FL on handling of personal data	RF	Average

* linking the account to the e-mail address is required. In this case, the user's data can be considered as personal data (PD)

** it is not explicitly stated in the user rules in VK that the requirements of the legislation of the Russian Federation for storing, transmitting and processing personal data are fulfilled (https://vk.com/privacy). The rules for protecting VK Connect user information are a part of the VK Ecosystem and contain links to 152-Federal Law.

Despite that, the number of users of these and similar services is estimated as tens and hundreds of thousands only in the Russian Federation. In the context of restrictions related to the spread of coronavirus, the requirements for the stability of services, as well as the requirements for compliance with Russian legislation in the field of personal data processing, become important [5].

Unfortunately, in most cases, these standards are not met. Table 2 shows the technical features of storing and processing user data, which according to [5] can be classified as personal data.Having analyzed the features of TDT in terms of storage and processing user data, and also the registration requirements, we selected some TDT that can be used by tutors and educational establishments at minimum cost and at low risk of violating the regulations of the Russian Federation relating to personal data processing:

- BigBlueButton webinar system. It is possible to install the system on the organization's own server or even on a teacher's personal computer (as was performed at the Department of Computer Engineering and Modeling of the Institute of Physics and Technical Sciences, Crimean Federal V. I. Vernadsky University). Students are not required to register and submit their personal data – to get connected they follow a link;
- AWWApp-interactive online whiteboard. Basic functionality (free illustrations, selection of tools, background loading of images and pdf-files, etc.) does not require registration for both teachers and students;

- using the functionality of the social network Vkontakte. Registration and confirmation of the phone number are required. At the same time, Vkontakte places its servers on the territory of the Russian Federation and declares compliance with the norms of 152-FL.

However, the TDT being under consideration, and many others are subject not only to the personal data information security threats but also to various other information security threats, which can occur any time.

4. Information security risks and equivalent damages

If the upper segment of the TDT (servers), communication channels, or lower-level devices (user devices) are affected by information and technical interference, there can occur a disruption of the educational process for some time. The examples of real problems that the participants of the educational process face are:

- inability to connect to the broadcast streaming;
- electronic services failure, lagging, etc.;
- indirect threats related to the leakage or deliberate misuse of the user's personal data by the service.

For an individual participant of the educational process, the above-mentioned issues may not be critical, but the number of people involved in the process can be substantial and can significantly (a hundredfold or even thousands of times) surpass the number of those people who are negatively affected by misfunctions of the automated control systems, classified as critical information infrastructure (in the commonly used meaning of this definition).

Some of the indicators for assessing the security of the automated systems are the probability (or frequency) of successful computer attacks (CA), that cause the transition of the system to a state of misfunction or failure (PCA_i), and the notional value of damage from a single CA (ξ_i), where i is the index of the CA kind and the damage corresponding to it. Risk is most often understood as the product of the following parameters:

$$R_{CA} = \sum_{i=1}^{N} \left(P_{CA,i} \cdot \xi_i \right), \tag{1}$$

The regulatory documents – All-Union State Standard and IEC on risks – contain a list of methodology for assessing the risk, such as: RIA, HAZOP, HACCP, SWIFT, and others [6]. A multidisciplinary approach can be applied to risk assessment, as risks can result from a wide range of causes and have a large number of consequences. However, in practice they are all qualitatively defined on the basis of brainstorming, expert experience, scenario analysis, etc.

As a result, in most cases in practice, the notion ‘damage’ is considered to be some notional value. At the same time, in jurisprudence, the damage is almost always assessed from both sides: material and moral, which, of course, have some financial equivalent [7].

To be able to compare risks, their characteristics should be comparable. First, we are going to consider automated control systems (ACS) and the impact that computer attacks have on them. We are going to deal with the risks that do not lead to human death (in order to avoid interference with the moral issue). All the same, such risks do damage to the health of the people involved in the critical information infrastructure functioning. Financial damage, in this case, can be expressed as the sum of the money paid off to each sufferer (N_O) to cover the costs of treatment c_i, temporary loss of labour capacity d_i, moral, or non-pecuniary, damage U_i, which, as has been said, can also be assessed in monetary terms, just as it happens in jurisprudence.

$$\xi_0 = \sum_{i=1}^{N_0} \left(c_i + d_i + U_i \right), \tag{2}$$

Non-pecuniary damage may be translated into a financial equivalent with some margin of error δ. Similarly, the harm done to the reputation and risks of the disruption of teacher's digital tools functioning lead to a "moral damage" for state bodies and the system of education, since the number of people affected is extremely large. Consequently, such reputational risks can also be assessed in

financial terms. What is more, additional financial resources are required to organize explanatory and other corrective work with the population in order to maintain the overall level of satisfaction at a certain level. The formula (3) for calculating the financial equivalent of the damage ξ_{IS} caused by the negative impact on the TDT is similar to (2):

$$\xi_{IS} = \sum_{i=1}^{N_{IS}} (c_i + d_i + U_i), \quad (3)$$

where the majority of i: $c_i, d_i \to 0$, however $N_{IS} >> N_o$.

When comparing the damage magnitudes ξ_O and ξ_{IS}, it is possible to note the main difference, which is the following: $N_{IS} >> N_o$. This leads us to the conclusion that in case of computer attacks on the information infrastructure used for educational purposes, the damage values ξ_O and ξ_{IS}, expressed in notional financial equivalent, are comparable in order of magnitude.

5. Conclusion

Based on the analysis of TDT, we can conclude that there is a wide range of such programs. At the same time, in terms of their compliance with Russian legislation on personal data protection and from the standpoint of so-called "digital sovereignty", the choice is significantly narrowed down to several programs. The basic parameters of a teacher's digital tools are presented in tables 1 and 2, but just a few of the products can be recommended.

The damage, expressed in the notional financial equivalent, done to a typical information system relating to objects of critical information infrastructure (CII) ξ_O and the damage to an information system used for educational activities – a teacher's digital tool ξ_{IS} – are comparable in order of magnitude.

Consequently, it becomes obvious that it is important to pay particular attention to TDT that should be easy to use, have minimal system requirements and, at the same time, provide a high level of protection from computer attacks and sanctions pressure.

6. References

[1] Federal State Educational Standard of Higher Education - Bachelor's degree in 09.03.01 Informatics and computer technology. Approved by order of the Ministry of Education and Science of the Russian Federation on September 19, 2017 No. 929.

[2] Ministry of Education and Science of the Russian Federation. Order of October 6, 2009 No. 413 "On the approval and implementation of the Federal State Educational Standard for General Secondary Education."

[3] Digital tools of the teacher. Experience of the Department of Computer Engineering and Modeling of the Physics and Technical Sciences Institute. 2020. URL: https://cfuv.ru/news/cifrovye-instrumenty-prepodavatelya-opyt-kafedry-kompyuternojj-inzhenerii-i-modelirovaniya-fiziko-tekhnicheskogo-instituta.

[4] Zoom is Leaking Peoples' Email Addresses and Photos to Strangers / Joseph Cox // Vice, 2020. URL: https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos.

[5] Federal Law "On Personal Data" of July 27, 2006 No. 152-FL.

[6] All-Union State Standard ISO / IEC 31010 - 2011 Risk management Risk assessment methods Moscow Standardinform 2012. Approved and put into effect by the Order of the Federal Agency for Technical Regulation and Metrology No. 680-st 4 of December 1, 2011.

[7] Ibragimova Aminat Ibragimovna Civil law essence and definition of the concepts of harm and loss // Problems of Economics and Legal Practice. 2013. No. 5. URL: https://cyberleninka.ru/article/n/grazhdansko-pravovaya-suschnost-i-opredelenie-ponyatiy-vreda-i-ubytkov.