Information Security and Online Education During the COVID-19 Pandemic

Gennadi B. Pronchev
Lomonosov Moscow State University

Inna V. Goncharova
Lomonosov Moscow State University

Aleksei P. Lyubimov
Presidium of the Russian Academy of Sciences
Diplomatic Academy of the Ministry of Foreign Affairs of Russia

Aleksander P. Mikhailov
Keldysh Institute of Applied Mathematics of the Russian Academy of Sciences

Relevance of the problem in question is associated with academics facing information threats in the virtual educational environment during the COVID-19 pandemic and the short-term transition of the education process to distance learning. We aim to analyze information threats to individuals in the Runet virtual educational environment and suggest measures to neutralize them. Research into this problem relies on a structural and comparative analysis as the theoretical approach. The empirical method of exploring this problem is an Internet-based study of user engagement in the Runet, focusing on cases in question and identifying the content that is most popular with the users. A classification of the current information threats is provided, and mechanisms for the elimination of emerging threats are discussed. Although Russia puts considerable effort, at the legislative level, into the prevention of malevolent information actions on academics, a number of particularities of virtual social environments allow for partial implementation of the measures only. The results may be of interest for specialists dealing with challenges of modern education, information warfare, information security of virtual social environments.

Keywords: virtual educational environments, the internet, COVID-19, information threats

INTRODUCTION

For the contemporary society, the COVID-19 pandemic has brought a large number of new tasks to be tackled (Pronchev & Sushko, 2021). One of them is the transition of educational institutions to an online training format (Sushko & Pronchev, 2021; Kuzembayeva et al., 2022; Soltovets et al., 2021). Given the time elapsed since the onset of the pandemic, this transition is no longer perceived as a temporary inconvenience (Cherepanova, 2020). Understandably, once the pandemic is over, distance learning will remain in active use simultaneously with conventional forms of training. Research has shown that there was a fairly high interest in distance learning present before the beginning of the COVID-19 pandemic (Pronchev et al., 2019). Consequently, online forms of training have to be developed in terms of methodology and didactics.

Currently, distance learning is viewed as the process of interaction between various individuals to transmit and receive new knowledge or explanations of scientific technical problems; its distinctive features are integration and the transfer of scientific knowledge and conventional forms of training into the digital environment (Monakhov & Pronchev, 2020). At present, one cannot obtain knowledge without using modern information, and communication technologies and virtual social environments are created on this basis (Pronchev et al., 2018). Similarly, a specific subject cannot be taught without addressing the relevant information and communication resources.

Although there are many advantages to using virtual social environments, the same environments bear serious risks. Results from a survey of Russian users' attitude to the aggressive content on social media have highlighted the respondents' negative attitude to such video clips posted in the media space. This reaction demonstrates that the audience is aware of the negative impact that aggressive content can have on people's mental sphere and social behavior (Goncharova et al., 2022).

The new risks which emerged during the COVID-19 pandemic are associated with an intensified globalization of the media space. As a consequence, there is an increase in cyberthreats to Russia in general, particularly to its citizens involved in this process. The international community, Russia included, needs to make efforts to ensure global cybersecurity worldwide. However, some countries took advantage of the difficulties experienced during the pandemic to wage information wars on their political opponents (Pronchev et al., 2021; Pronchev & Mikhailov, 2021).

Virtual social environments of the Runet are the major source of information for the majority of young Russian individuals, who are the most active internet users. According to research by Osipova et al (2018), "of all kinds of the Mass Media, the vast majority (93.9%) of students (95.5% of junior bachelor-degree students, 93.8% of senior bachelor-degree students, and 91.1% of master-degree students) prefer various Internet-based mass media to television (4% overall; 2.7% of junior bachelor-degree students, 4.8% of senior bachelor-degree students, and 5.6% of master-degree students). Listening to the radio and reading printed periodicals were the options preferred by a insignificant number of study participants. In most cases, the Internet is used for communication (91.9%), researching information (90.7%), entertainment (73.3%), studies (67.4%), work (43.1%), and gaming (11.5% (Osipova et al., 2018)."

In general, individuals using digital space must have a respectful attitude towards other users, themselves, the information and technological processes, and the hardware. Additionally, they should have a sense of duty and responsibility and render friendly support (Goncharova & Pronchev, 2015; Monakhov et al., 2018). These qualities will reduce the disruption of the digital educational and scientific environment (Strielkowski & Chigisheva, 2019; Soltovets et al., 2020).

Similar to moral upbringing, digital upbringing is formed within a consistent system of the educational process. Students "do not create any notions, patterns, values, or standards of the public moral, but they adopt ones in the process of their academic activities. While being engaged in them, they perform mental actions that are relevant to those by which the said products of spiritual life were generated historically" (Davydov, 1986). Such an understanding is represented in technical specifications, scientific papers, and educational standards concerning questions of information security.

LITERATURE REVIEW

The Pedagogical encyclopedic dictionary provides the following definition: "Distance learning is a technology of focused and methodologically organized management of academic and cognitive activity of students living away from the educational center (regardless of the level of education they are getting). Distance learning is performed using means and methods of pedagogical communication between teachers and students with the minimum number of compulsory classes. In its methods of organization of the educational process, distance learning is close to the extramural form of training, while the saturation and tempo of the educational process bring it close to intramural studies" (Dictionary, 2002).

Advantages of distance training are a flexible schedule and the absence of location attachment. As for its disadvantages, there is no methodologically considered technology of building the academic activities based on distance learning, information security issues arise for all participants of the process, etc. (Pronchev et al., 2019).

The concept of informatization in education is associated with education globalization issues aimed at aligning national traditions and technologies of training and elaborating uniform educational standards. This is rendered possible due to the rapid development of information technologies (Goncharova et al., 2017).

For example, the digital library of the Dutch Association for Computer Machinery disposes a large amount of literature on cybersecurity programs for children (ACM, 2021). The CSTA K-12 CS standards (K12, 2017) list the competencies that need to be acquired by students of elementary and high schools before they can claim computer knowledge. Many countries have adopted these standards as the basis of the curricula (Duncan & Bell, 2015). Therefore, for school-aged children older than elementary grades, there is a free-access curriculum available on Code.org, CS Discoveries, which covers a range of topics on programming, physical computing, HTML/CSS, and data (Code, 2018). The AP CS Principles course, which is targeted at children in later stages of their school education, extends their knowledge up to core computer concepts (Cuny, 2015). Alongside the availability of the above resources, digital library of the Dutch Association maintains live exchange of innovations and experiments for computers (Riel & Romeike, 2020; Bernd et al., 2022). On top of this, to study cybersecurity, one can choose from 85 gaming educational tools available (Maqsood & Chiasson, 2021).

Questions regarding the effectiveness of teaching cybersecurity in Western countries such as the Netherlands, and the way it influences children’s behavior in cybersecurity, were discussed in a study by Witsenboer et al (2022). The authors concluded that students in the Netherlands do not develop their cybersecurity skills efficiently at elementary and high school. The students shared their cybersecurity experiences relating to e-mails, passwords, phishing, and physical blocking of their devices; however, many students also developed self-assurance and reckless behavior in terms of Internet usage and messages regarding online incidents. The students noted that school had not played much part in developing their cybersecurity skills. They learned this behavior mainly through experience, manuals available on the Internet, and with the help of parents and siblings (Witsenboer et al., 2022).

Meanwhile, there is an urgent necessity to regulate the main principles of training. The use of modern educational platforms based on virtual social environments enables the differentiation between the concepts of distance learning and extramural studies. Distance learning implies holding classes online in real-time using interactive teaching techniques and materials (Goncharova et al., 2017). In this way, one can discuss the technological effectiveness of the educational process. An important aspect is associated with fulfilling the accessibility requirement and ensuring that there is no educational inequality (Pronchev et al., 2018). All students and teachers must have similar and equal opportunities to access devices and applications: educational platforms, resources, or other teacher-student communication technologies. Alongside this, the educational process is wide-scale. The devices used must be well known to a wide range of users, and communication apps, educational platforms or resources must be designed for a broad audience, with their age-related features catered for. Distance learning must be configured based on the standards of computer exposure time for users of different age categories, specifically, for school-aged children. Particular attention must be paid to the correct organization of the workspace. Following this, the principle of health promotion must be adhered to. When transitioning to the online format, it is important to keep the fundamental didactic principles unchanged: the scientific character, accessibility, focus, systemic and consistent character, illustrative purpose, and coherence of training (Goncharova & Pronchev, 2020).

Information security is a crucial problem in the transition to e-learning using distance educational technologies. Information risks associated with operating in virtual social environments are also present in the educational environments (Pronchev & Goncharov, 2017; Pronchev et al., 2020). First, this directly applies to academic and methodological information and second, it impacts the personal and confidential information of the individuals using the education process. The information can be stolen, damaged, modified, or removed.

Notably, possible consequences of actions unauthorized by the teacher differ greatly for the first and second information types. While the former type can lead to temporary difficulties in the organization of the education process and assessment of the students' actual knowledge, the latter type involves problems with people's safety as a consequence (Pronchev & Goncharov, 2017).

Concerning the second information type security problem in virtual social environments, Korablev et al. (2010) provided a classification of possible threats according to confidentiality, integrity, accessibility, completeness, relevance, importance, targeting, and redundancy of the information. They also identified potential intruders and suggested an information and logical model of protection of confidential information in virtual social environments (Korablev et al., 2010).

Information security can be characterized as a system of measures used to protect academic, methodological, and personal information from being stolen, and prevent hacking attacks that aim to tamper with the system configuration. It also protects the educational process against dissemination of prohibited information, such as pornography, promotion of violence, and involvement into criminal structures, etc.

Information threats can be deliberate and unintentional in nature; therefore, technical hardware problems, crashes, and communication system failures belong to the latter. Deliberate threats include, among other matters, third party hooliganism. For example, unauthorized hackers disrupting academic video conferences with porn get a broad coverage (Runev, 2020). Hackers can gain unauthorized entry directly via access to the server or computer, and subsequently release information to external media. They can also use special software to hack, copy, and intercept information and technical devices, depending on their goals.

At present, there are some technical devices that have been successfully used to ensure the integrity of information systems. Among these are the specialized software products, e.g., DLP and SIEM systems; however, these are expensive (Kulagina, 2016). Antivirus software is in broad use, and its effectiveness varies depending on the programs.

Within the set of information protection measures, the administrative procedures of an educational institution specify its internal rules and processes for handling information. Physical restriction measures, suggesting an access control system with different level permits to enter computer classrooms, can also be referred to.

RESEARCH METHODOLOGICAL FRAMEWORK

The objective of this research is to analyze information threats to individuals using virtual educational environments and suggest measures to curb them.

Due to the COVID-19 pandemic and the transition of Russia's educational process to e-learning, and therefore an extensive use of the online mode, information security of these users has become urgent.

Objectives of this research are as follows:

1. To determine the information threats to users of the Runet virtual educational environments.
2. To analyze Russian regulatory documents governing information security in virtual educational environments.
3. To conduct an empirical Internet study of the Runet user engagement into the problems in question and to find out the users most preferred content.
4. To describe suggestions to curb the threats persisting in the Runet virtual educational environments.

Research into the stated problem relies on structural and comparative analysis as the principal theoretical approach. An Internet user engagement study that focuses on the cases in question and identifies the content which is the most popular with the users, provides the basis for an empirical study.

In this work, the Internet study conducted by the authors on November 01, 2021, was used as the source of empirical data. Previously, the authors evaluated the technology using the Popsters analytical multi-functional tool in sociological surveys and found that it correlated with classical quantitative research methods (Pronchev et al., 2020).

The Internet study hypothesized that there was a stable and significant statistical association between user activity in the Internet communities and a particular topic (descriptors), and the level of significance of the selected topic for them (indicators) (Petrov & Pronchev, 2017; Pronchev et al., 2019).

The Popsters analytical service (Online: https://popsters.ru. Available November 01, 2021) was used as a toolkit. Various metrics of the Popsters resource were employed (Table 1).

TABLE 1
THE POPSTERS RESOURCE METRICS

Metric name		**Description**
ER		Users' engagement rate of the content published (**posts**)
	ER post	Users' engagement rate of particular posts **ER post = (likes + reposts + comments [+ dislikes for YouTube]) / quantity of followers**
	ER day	Total users' engagement rate for all posts published within a day
	ER view	Engagement rate of a particular post calculated as the number of views (for VKontakte, YouTube, Coub, and Flickr) **ER view = (likes + reposts + comments [+ dislikes for YouTube]) / quantity of views of the published item**
	Average ER post	The arithmetic average of ER post for all published items for the period under analysis
	Average ER view	The arithmetic average of ER view of all the posts
	Average ER day	The arithmetic average of ER day for the entire period under analysis
LR		Love rate (**"likes" only**) **LR = (The total number of likes) / quantity of followers / quantity of published items for the period under analysis**
TR		Talk rate (**comments only**) **TR = (The total number of comments) / quantity of followers / quantity of published items for the period under analysis**

ER: Engagement rate, LR: Love rate; TR: Talk Rate. Source: (Pronchev et al., 2020)

Thus, ER (Engagement rate) displays the percentage of users who were active in publications. ERpost is an average engagement in a specific post in the community. Average ER post is an average engagement by posts in the community for a certain period. Obviously, it is significantly lower than ER.

Regrettably, but to date, there is no scientifically substantiated concept combining digital upbringing and training, online learning included. To implement such a large-scale project, one has to scrutinize the attitudes of participants of virtual social environments to the ethical aspect of online information security. In particular, the opinions of social media users have to be studied.

RESULTS AND DISCUSSION

The mathematical model of information propagation in virtual social environments (Mikhailov et al., 2018; Petrov et. al., 2022), which is basically a network information propagation model, was justified in terms of sociology. Its sociological substantiation has shown that there are a number of specific features that virtual social environments possess that only partially help make up for the legislative efforts of the government. These efforts are aimed at preventing malevolent information action on its citizens on the Internet (Pronchev et al., 2020).

More specifically, in the Russian Federation (RF) at the state level, information protection measures are governed by the regulatory framework relying on the Constitution of the RF (Constitution, 1993) and some other basic statutory instruments. Among the latter, the following should be named: Federal law of December 28, 2010, No. 390-FZ “On security” (FZ, 2010), Federal law of July 27, 2006, No. 149-FZ “On information, information technologies, and information protection” (FZ, 2006a), and Federal law of July 27, 2006, No. 152-FZ “On personal data” (FZ, 2006b). The “Strategy of national security of the Russian Federation” approved by the Decree of the President of the Russian Federation on December 31, 2015, No. 683 (Decree, 2015), the “Doctrine of information security of the Russian Federation” approved by the Decree of the President of the Russian Federation on September 9, 2000, No. 646 (Decree, 2016), and some other enactments should also be mentioned. All other subsequent instruments were aimed to ensure the above documents were more specific and implemented (Lyubimov, & Shchitov, 2017).

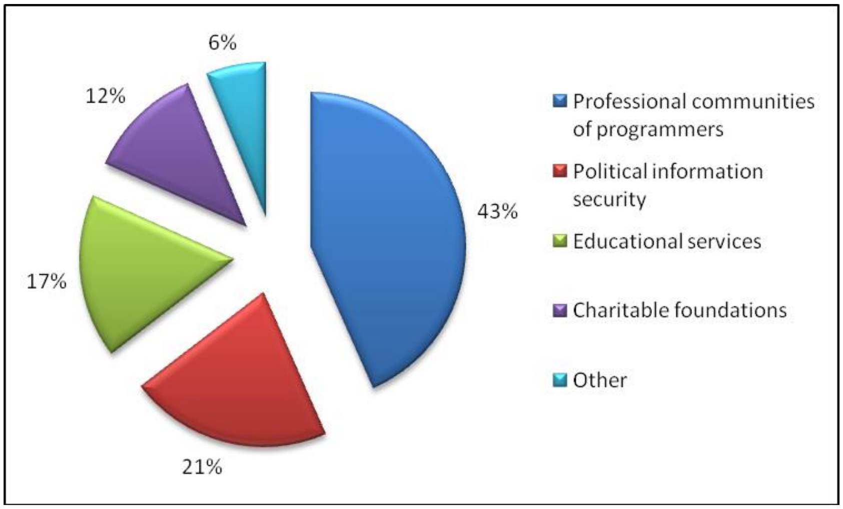
Alongside the above, copyright and database rights have to be adhered to. The means of social and ethical information security provision are a set of measures which is currently incipient. Social and ethical standards must be viewed within the context of preventing deviant behavior in virtual social environments (Pronchev, 2020). For the first time in human history, it is not the older generation who is teaching the young; conversely, it is the younger generation who have the state-of-the-art technical knowledge. The virtual space is that of the younger generation who are not always prepared to accept responsibility for their actions. Moreover, a sense of impunity is created resulting in deviations of various kinds (Pronchev, 2020).

To identify information threats to users of the Runet virtual educational environments, an empirical study was conducted on November 01, 2021.

The “Information security” query retrieved from the Vkontakte social network showed that there were 4688 communities registered on this social network, with the "Hacker / xakep.ru – hacking, security and protection" group having the greatest number of subscribers (n=195,065).

The Internet-based communities can be conventionally subdivided into several groups according to their content type. For example, professional communities of programmers and information security specialists, political information security, educational services of various focus, and charitable funds (Figure 1).

FIGURE 1
DISTRIBUTION OF INTERNET COMMUNITIES ACCORDING TO THE CONTENT TYPE (%)



For further analysis, we used the Popsters (popsters.ru) resource and explored the users’ activity for the set topics between the 29th of September 2021 and 30th of October 2021.

All groups were considered when analyzing the professional community. The communities with more than 10,000 subscribers are listed in Table 2.

TABLE 2
INTERNET COMMUNITIES WITH MORE THAN 10,000 SUBSCRIBERS

Communities (transcribed titles)	Translated titles (meaning)	No. of subscribers	No. of views	Average ERpost (%)
Khakery | Etichniy khaking s Mikhailom Tarasovym https://vk.com/public44038255	Hackers | Ethical hacking with Mikhail Tarasov	12,508	61,561	0.23
PSH-WORLD | Informatsionnaya Bezopasnost https://vk.com/public3457574	PSH-WORLD | Information security	21,668	1,223	0.16
Sluzhba podderzhki – Vkhod.ru https://vk.com/public42119847	Vhod.ru support desk	46,186	22,406	0.02
Khaker / xakep.ru — vzlom, bezopasnost i zashchita https://vk.com/public10933209	Hacker / xakep.ru – hacking, security, and protection	195,065	99,723	0.01
overpublic1 https://vk.com/public79759696		133,272	821,554	0.21
Razrabotka iOS, Android, WEB App. Namasam IT https://vk.com/public53773933	iOS, Android, WEB App development. Namasam IT	11,681	0	0
RTM Group | IT-eksperty i yuristy | Audit IB https://vk.com/public11189040	RTM Group | IT experts and lawyers | IS audit	12,235	1,228	0
GreyTeam | Khakery https://vk.com/public169106523	GreyTeam | Hackers	11,286	359,390	0.62
Informatsionnaya Bezopasnost https://vk.com/public69741303	Information security	10,013	2,282	0.32
The Codeby https://vk.com/public75857525		10,005	162,476	0.36

ER: Engagement Rate; No: Number

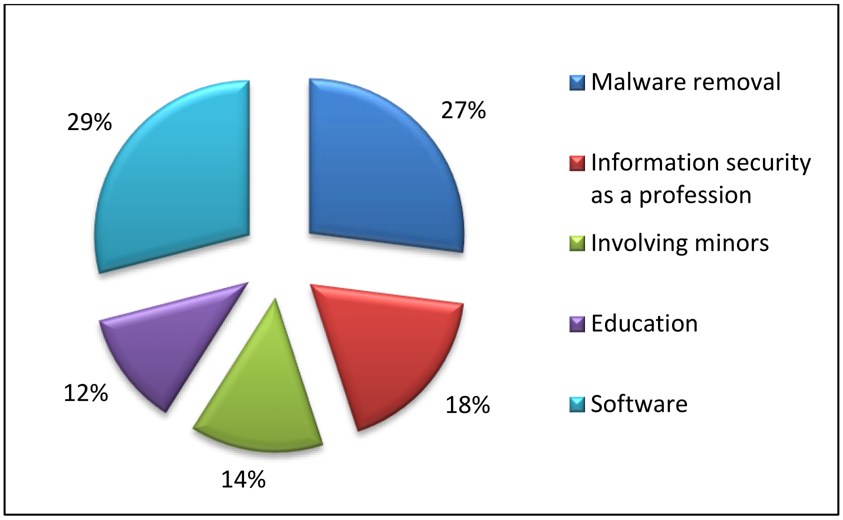
The user activity in communities, such as their likes, comments, reposts, and engagement rates, can be used to determine various ratings.

The post “Hacking by examples” by the “Hackers | Ethical hacking with Mikhail Tarasov” community and the post by GreyTeam| Hackers, can be noted according to their ER post engagement rate, which is 2.99% and 2.03% respectively. The ER post engagement rate is calculated as the quotient of the sum of likes, reposts, and comments and the number of subscribers or users of the content posted. The former post is a presentation of A. A. Yaroshenko’s book “Hacking by examples. Vulnerabilities, hacking, protection” (Yaroshenko, 2021); the latter is a meme with the slogan “Enough cranking out Trojans and RATs”.

In general, it is short text that prevails in professional communities making up to 80% of the total of content. Brief meme posts are the most numerous; the comic effect of various information security breaches and faults is discussed in the professional slang (73%).

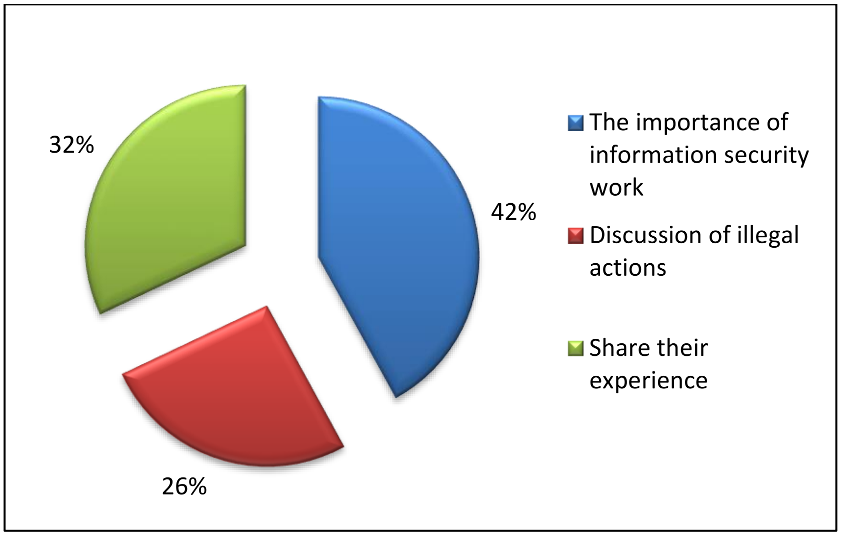
The subscribers were actively discussing posts which can be conventionally subdivided into further categories (Figure 2).

FIGURE 2
DISTRIBUTION OF COMMENTS ACCORDING TO TOPICS (%)



In their comments to the posts, the users focus on the importance of work, issues arising, and share their experience. They communicate in slang which is clear to programmers and information security specialists.

FIGURE 3
CONTENT OF COMMENTS (%)



In the discussion topic on the involvement of minors, the post by The Codeby community is of note (Codeby, 2021). It tells the story of an app that faked the Ukrainian Diya, enabling schoolchildren to buy spirits and cigarettes by doctoring their age in the electronic passport. Payments for the fake Diya were collected directly to the bank account of the author of the app. This was unwise. The 21-year-old app developer from Ukraine, was identified and arrested, and is facing up to six years in prison (Codeby, 2021).

In the comments it becomes clear that the users of this community disapprove of such actions; they doubt, however, that it was the actual developer who the authorities found (Codeby, 2021).

Thus, it can be assumed that the professional community condemn all forms of cracking, illegal actions, and hacking, and unites around the idea of information security.

When analyzing educational communities, we considered all groups. The communities with more than 5,000 subscribers are listed in Table 3.

TABLE 3
EDUCATIONAL INTERNET COMMUNITIES WITH MORE THAN 5,000 SUBSCRIBERS

Communities (transcribed titles)	Translated titles (meaning)	No. of subscribers	No. of posts	No. of views	Average ERpost (%)
Life-Hack / Zhizn-Vzlom https://vk.com/public163703907	Life-Hack / Hacking Life	24,319	115	670,205	1.76
Akademiya energo-informatsionnoy bezopasnosti https://vk.com/public115516032	Academy of energy and information security	23,147	16	1390	4.14
OTUS. Onlain-obrazovanie https://vk.com/public145052891	OTUS. Online education	10,457	133	79848	0.56
PSH-WORLD | Informatsionnaya Bezopasnost https://vk.com/public3457574	PSH-WORLD | Information security	21,666	1	405	6.67
Informatsionnaya bezopasnost https://vk.com/public69741303	Information security	10,014	1	1,811	2.37
Rostovskiy kolledzh svyazi i informatiki (RKSI) https://vk.com/public75021	Rostov-on-Don College of Communica-tion and Informatics	7,025	40	90,303	1.02
Kiberdruzhina Volgogradskaya oblast https://vk.com/public138547391	Cybersquad of Volgograd Region	5,862	3	646	3.99
Pentestit https://vk.com/public40086034		5,716	1	2,356	0.55

ERL Engagement Rate; No: Number

Table 4 presents the top 10 popular topics (according to the number of views) among users.

TABLE 4
POST TOPICS MOST POPULAR WITH USERS
(ACCORDING TO THE NUMBER OF VIEWS)

Post topics	Number of views
Fighting against counterfeited QR codes	48,730
Creating a fake page with porn content	37,601
Changing technical devices to provide law enforcement intelligence functions	27,332
A copper cable stolen by a hacker	27,116
Samsung apologized for Russian software on Britons’ smartphones	26,533
Android phones keep watching their users	25,231
An American hacked the flying school system to revenge on her ex	23,085
Microsoft admitted some Windows users could face network printer issues	19,267
A nuclear power engineer’s spy plans revealed by an undercover FBI agent	14,396
The new malware AbstractEmu roots Android mobile devices	14,010

Table 5 provides the top 10 approved posts (according to the number of likes).

TABLE 5
POST TOPICS MOST APPROVED BY USERS (ACCORDING TO THE NUMBER OF LIKES)

Post topics	Number of likes
Hacking any system using a USB	124
Classes cancelled due to the pandemic	107
Ten search engines hackers use	106
Hacking Windows 10	105
Creating a port scanner with Python	89
Exploiting routers using Routersploit	84
How to find and remove malware from Linux	79
Linux fundamentals for beginner hackers	78
Sixteen services to get information for free	73
How to hack wireless passwords	68

Table 6 lists the 10 post topics most shared by users for others.

TABLE 6
MOST SHARED POST TOPICS

Post topics	Number of reposts
Hacking any system using a USB	177
Ten search engines hackers use	137
Classes canceled due to the pandemic	131
Exploiting routers using Routersploit	123
Hacking Windows 10	118
How to hack wireless passwords	105
Linux fundamentals for beginner hackers	102
Creating a port scanner with Python	96
Collecting information from various sources	81
Sixteen services to get information for free	80

Table 7 lists the 10 posts that achieved the highest user engagement rate ERpost (%).

TABLE 7
POST TOPICS ACHIEVING THE HIGHEST USERS' ENGAGEMENT RATE

Post topics	ERpost (%)
Classes canceled due to the pandemic	3.39%
Hacking any system using USB	1.25%
Breakfast with the director	1.01%
Ten search engines hackers use	1.00%
Hacking Windows 10	0.92%
Exploiting routers using Routersploit	0.85%
Ten-day Festival of the Aged People, Remembrance Day of Participants of the Great Patriotic War	0.81%
Creating a port scanner with Python	0.76%
How to hack wireless passwords	0.74%
Linux fundamentals for beginner hackers	0.74%

Source: the authors (Popsters.ru)

Table 8 lists the 10 posts that had the largest number of comments written by users. Characteristics of the comments is also given in the table to describe the users' attitude to the topics.

TABLE 8
MOST COMMENTED POST TOPICS

Post topics	Number of comments	Description of comments
Fight method for fake QR-codes invented in Russia: Novosibirsk Pro Control team developers created a copy-protected QR code with a two-factor verification system	22	The tone of the comments was negative. The technology is imperfect, easy to hack, and there are no devices to scan such codes. Development of this technology looks more like using up the allocated budget funds. Such a technology will only complicate life for ordinary citizens.
A 10 mln rubles copper cable stolen by a Voronezh hacker	20	The tone of the comments was positive. The users condemn the hacker's actions, but they wonder what exactly the 10 mln rubles "copper cable" could be made of.
Head of Rosfin monitoring: terrorists got funded through currency in computer games	16	The tone of the comments was positive. The users make no question of the idea about financial support of terrorists via computer games. However, there are opinions about the state control of the gaming industry for further taxation purposes.
Android phones keep watching their users	16	The tone of the comments was positive. The users are worried and condemn personal data collection via smartphones.
Samsung apologized for Russian software on Britons' smartphones	11	The tone of the comments was neutral.
Changing technical devices to provide law enforcement intelligence functions	10	The tone of the comments was negative: they speak about using up the budget funds.
How to hack wireless passwords	7	The tone of the comments was neutral: the post is discussed in terms of profession.
Roskomnadzor is going to fine Google 22 bln rubles	7	The tone of the comments was negative. The users do not support the decision of the Russian Federal Service for Supervision in the Sphere of Telecom, Information Technologies, and Mass Communications.
Microsoft admitted some Windows users could face network printer issues	6	The tone of the comments was negative.
The alleged Twitter hacker is charged with $784,000 for theft of cryptocurrency by SIM-card exchange	5	The tone of the comments was neutral. The users wonder how the hacker could accomplish it all on his own.

Summing up the empirical data collected, the following results have been obtained:

- The posts are brief and informative in nature, and the text is short in length.
- In all rated categories, overlapping of posts is observed.
- There is a major gap between the number of views and other categories of the rating.

- Although the group of communities was referred to as the educational unit, users posts focused on the general information security topic not related to education.
- Feedback can be traced by the post ER.
- Although the number of comments is few, the users' opinion and tone of their messages can be determined.
- The users disapprove of hackers' actions. They support expedient solutions in information security and reasonable spending of budget funds. The disapprove of personal data collection without consent.

Substantial work is required to create a code of ethical rules for using information and communication technologies aimed at digital moral education of young people, which would also consider international traditions. UNESCO's Code of Ethics for the Information Society (Ethics, 2011) can be noted as an example.

Digital education must rely on the prevailing definition which is the "activity aimed at developing personality, creating conditions for students' self-identification and socialization based on sociocultural, spiritual, and moral values, and rules and standards of conduct accepted in the society for the benefit of the people, family, society, and state" (FZ, 2012).

The introduction of young people to the information security problem fulfills the underlying principles of moral education and provides solutions for the following tasks:

- First, establish the coordination of the digital education process with academic and scientific activities, which are increasingly becoming more e-focused, and transfer this into the virtual space.
- Second, create a microclimate for young people to fully access the social virtual space and provide conditions which allow them to become established as moral people who maintain clear online behavior principles and recognize their responsibility for the future development of the virtual space and technologies.
- Third, develop the young people's professional e-competency within the context of the overall digital worldview.
- Fourth, provide measures to support the initiatives of young, creative people and talents while also fulfilling an individual approach in the pedagogical work.

CONCLUSION

As training shifted to virtual social environments, the COVID-19 pandemic brought new information threats to the participants of the education process.

The Russian public disapproves of an intruders' actions in virtual social environments.

At the legislative level, Russian state authorities put considerable effort into the prevention of malevolent information actions on participants of the Runet-based virtual education process; nevertheless, there are a number of specific features of virtual social environments that allow for partial implementation of the measures only. Even so, the state must continue working on this vision.

Extensive work is also required to create a code of ethics in the sphere of using virtual educational environments aimed at digital moral upbringing of young people.

As a mechanism of combating information threats, the level of competence of virtual educational environment users (both students and teachers) has to be improved.

ACKNOWLEDGEMENT

This research was supported by the Russian Science Foundation (project no. 20-11-20059, Keldysh Institute of Applied Mathematics RAS).

REFERENCES

ACM. (2021). ACM Digital Library. Retrieved from https://dl.acm.org

Bernd, J., Garcia, D., Holley, B., & Johnson, M. (2022). Teaching Cybersecurity: Introducing the Security Mindset. In *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 2* (SIGCSE 2022). Association for Computing Machinery, New York, NY, USA, 1195. https://doi.org/10.1145/3478432.3499160

Cherepanova, Y. (2020). Between the first and second: Online education in the wake of a pandemic. *Forbes Education*. Retrieved from https://education.forbes.ru/authors/online-education-vs-covid

Code. (2018). *CS Discoveries Curriculum Guide 2018-2019*. Retrieved from https://curriculum.code.org/csd-18

Codeby. (2021). *What do you know about anonymity? The Codeby*. VK.COM. Retrieved from https://vk.com/wall-75857525_9939

Constitution. (1993). Russian Constitution. Adopted by popular vote on December 12, 1993, with changes approved in the all-Russian vote on July 1, 2020. Retrieved from http://kremlin.ru/acts/constitution

Cuny, J. (2015). Transforming K-12 computing education: AP® computer science principles. *ACM Inroads*, *6*(4), 58–59. https://doi.org/10.1145/2832916

Davydov, V.V. (1986). *Problems of developing learning: The experience of theoretical and experimental psychological research*. Moscow: Pedagogy.

Decree. (2015). *Decree of the President of the Russian Federation of December 31, 2015 No. 683*. Retrieved from http://www.kremlin.ru/acts/bank/40391

Decree. (2016). *Decree of the President of the Russian Federation of December 05, 2016 No. 646.* Retrieved from http://www.kremlin.ru/acts/bank/41460

Dictionary. (2002). Pedagogical Encyclopedic Dictionary. Ch. ed. B.M. Bim-Bad. Moscow: Big Russian Encyclopedia.

Duncan, C., & Bell, T. (2015). A pilot computer science and programming course for primary school students. *Proceedings of the Workshop in Primary and Secondary Computing Education* (WiPSCE’15), pp. 39–48. ACM, New York, NY. https://doi.org/10.1145/2818314.2818328

Ethics. (2011). Code of Ethics for the Information Society proposed by the Intergovernmental Council of the Information for All Program (IFAP). *UNESDOC*. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000212696

FZ. (2006a). Federal Law No. 149-FZ of July 27, 2006 “On Information, Information Technologies and Information Protection”. Retrieved from http://www.kremlin.ru/acts/bank/24157

FZ. (2006b). Federal Law No. 152-FZ of July 27, 2006 “On Personal Data”. Retrieved from http://www.kremlin.ru/acts/bank/24154

FZ. (2010). Federal Law No. 390-FZ of December 28, 2010 “On security”. Retrieved from http://www.kremlin.ru/acts/bank/32417

FZ. (2012). Federal Law No. 273-FZ of December 29, 2012 “On Education in the Russian Federation”. Retrieved from http://www.kremlin.ru/acts/bank/36698

Goncharova, I.V., & Pronchev, G.B. (2020). Regulation of the basic principles of distance learning in the context of the covid-19 pandemic. COVID-19 as a factor of reflection of social inequality. *International Scientific Conference. Collection of materials*, pp. 61–63. Moscow: MAX Press. Retrieved from https://www.socio.msu.ru/documents/20210111_sbornik.pdf

Goncharova, I.V., P & Ronchev, G.B. (2015). Moral education of young people in the context of helping people with disabilities. *Education and Upbringing*, *2*, 66–69.

Goncharova, I.V., Pronchev, G.B., & Tretyakova, I.V. (2017). Innovations in the field of mathematical and information training of sociology students in the context of globalization processes. *Education and Law*, *8*, 241–253.

Goncharova, I.V., Pronchev, G.B., Rodionova, M.E., & Krichever, E.I. (2022). Runet users' attitude to the outrageous content in virtual social environments. *Academic Journal of Interdisciplinary Studies*, *11*(1), 258–268. https://doi.org/10.36941/ajis-2022-0023

K12. (2017). *K–12 Computer Science Framework*. Retrieved from https://k12cs.org/

Korablev, M.N., Lontsov, V.V., & Pronchev, G.B. (2010). Protection of confidential information in Internet social networks. *Sociology*, *4*, 33–45.

Kulagina, T. (2016). How information is protected in Russia. *RUNET*. Retrieved from https://runet.news/articles/7960

Kuzembayeva, G., Umarova, A., Maydangalieva, Z., Gorbatenko, O., Kalashnikova E., Kalmazova, N., & Chigisheva, O. (2022). Content and language integrated learning practices in Kazakhstan secondary schools during COVID-19 pandemic. *Contemporary Educational Technology, 14*(2), ep362. https://doi.org/10.30935/cedtech/11733

Lyubimov, A.P., & Shchitov, A.N. (2017). RGAIS-the leader in the profiles of training in the field of protection of intellectual property rights. *Representative Power-XXI Century*, *4*, 18–20.

Maqsood, S., & Chiasson, S. (2021). Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens. *ACM Trans. Priv. Secur*., *24*(4), 28. https://doi.org/10.1145/3469821

Mikhailov, A.P., Petrov, A.P., Pronchev, G.B., & Proncheva, O.G. (2018). Modeling a Decrease in Public Attention to a Past One-Time Political Event. *Doklady Mathematics*, *97*(3), 247–249. https://doi.org/10.1134/S1064562418030158

Monakhov, D.N., & Pronchev, G.B. (2020). From a digit to the digital society. *Political Science Issues*, *10*(3), 277–284. https://doi.org/10.35775/PSI.2020.42.3.002

Monakhov, D.N., Goncharova, I.V., & Pronchev, G.B. (2018). Information systems on the basis of modern information and communication technologies as a tool for the formation of leadership qualities. In *Leadership for the Future Sustainable Development of Business and Education*, *Springer Proceedings in Business and Economics* (pp. 521–529). https://doi.org/10.1007/978-3-319-74216-8_52

Osipova, N.G., Sinykov, A.V., Elishev, S.O., Kanevsky, P.S., & Trofimov, S.V. (2018). *A social portrait of the modern Russian student*. By results of a research at sociological faculty of Lomonosov Moscow State University. Moscow: FGBUN ISPI of RAS.

Petrov, A.P., & Pronchev, G.B. (2017). Collection of empirical data for the model of dynamics of interest in a political event. *Mathematical Modeling of Social Processes*, *19*, 75–79. Moscow: Keldysh Institute of Applied Mathematics RAS. Retrieved from http://keldysh.ru/social/2016

Petrov, A.P., Podlipskaia, O.G., & Pronchev G.B. (2022). Modeling the dynamics of public attention to extended processes on the example of the COVID-19 pandemic. *Computer Research and Modeling*, *14*(5), 1131–1141. https://doi.org/10.20537/2076-7633-2022-14-5-1131-1141

Pronchev, G.B. (2020). On the features of virtual social environments contributing to social deviations. *Education and Law*, *3*, 200–208. https://doi.org/10.24411/2076-1503-2020-10334

Pronchev, G.B., & Goncharov, I.V. (2017). Security of modern electronic educational environments. *Distance and Virtual Learning*, *3*, 26–30.

Pronchev, G.B., & Mikhailov, A.P. (2021). Particularities of genesis and functioning of the deep state within various political regimes. *AD ALTA: Journal of Interdisciplinary Research*, *11*(2-XXIII), 142–146.

Pronchev, G.B., & Sushko, V.A. (2021). Influence of the coronavirus pandemic on social processes in Russia. *AD ALTA: Journal of Interdisciplinary Research*, *11*(1), 310–315.

Pronchev, G.B., Goncharova, I.V., & Proncheva, N.G. (2020). The range of communication topics of the visually impaired in the internet communities. *Humanities and Social Sciences Reviews*, *8*(4), 301–314. https://doi.org/10.18510/hssr.2020.8431

Pronchev, G.B., Goncharova, I.V., Pronchev, K.G., & Krichever, E.I. (2019). Russians' attitude to distance learning: A Runet survey. *International Journal of Learning, Teaching and Educational Research*, *18*(11), 370–384. https://doi.org/10.26803/ijlter.18.11.22

Pronchev, G.B., Mikhailov, A.P., Lyubimov, A.P., & Solovyev, A.A. (2020). Particularities of the internet-based virtual social environments within the context of information warfare. *EurAsian Journal of BioSciences*, *14*, 3731–3739.

Pronchev, G.B., Monakhov, D.N., Proncheva, N.G., & Mikhailov, A.P. (2018). Contemporary virtual social environments as a factor of social inequality emergence. *Astra Salvensis*, *6*, 207–216.

Pronchev, G.B., Proncheva, N.G., & Goncharova, I.V. (2019). Modern management of media environment: Negative effects for the society of today. *Journal of Environmental Treatment Techniques*, *7*(4), 836–840.

Pronchev, G.B., Shisharina, E.V., & Proncheva, N.G. (2021). Cyber threats to modern Russia in the context of the coronavirus pandemic. *Political Science Issues*, *11*(1), 26–34. https://doi.org/10.35775/PSI.2021.48.1.003

Riel, M., & Romeike, R. (2020). IT security in secondary CS education: is it missing in today's curricula? A qualitative comparison. In *Proceedings of the 15th Workshop on Primary and Secondary Computing Education (WiPSCE '20)*. Association for Computing Machinery, New York, NY, USA, Article 35, 1–2. https://doi.org/10.1145/3421590.3421623

Runev, I. (2020). In Moscow, students were shown porn in a remote lesson. *KP.RU*. Retrieved from https://www.kp.ru/online/news/3838914

Soltovets, E., Chigisheva, O., & Dmitrova, A. (2020). The role of mentoring in digital literacy development of doctoral students at British universities. *Eurasia Journal of Mathematics, Science and Technology Education*, *16*(4), em1839. https://doi.org/10.29333/ejmste/117782

Soltovets, E., Chigisheva, O., Dubover, D., & Dmitrova, A. (2021). Russian digital education landscape during the current pandemic: is the impact felt? *E3S Web of Conferences*, *273*, 12026. https://doi.org/10.1051/e3sconf/202127312026

Strielkowski, W., & Chigisheva, O. (2019). Research and Academic Leadership: Gaming with Altmetrics in the Digital Age. *Springer Proceedings in Business and Economics*, pp. 307–313.

Sushko, V.A., & Pronchev, G.B. (2021). Online learning in the context of pandemic in Russia. *Revista Romaneasca Pentru Educatie Multidimensionala*, *13*(2), 1–17. https://doi.org/10.18662/rrem/13.2/407

Witsenboer, J., Sijtsma, K., & Scheele F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. *Computers & Education*, *186*, 104536. https://doi.org/10.1016/j.compedu.2022.104536

Yaroshenko, A.A. (2021). *Hacking by examples. Vulnerabilities, hacking, protection*. St. Petersburg: Science and Technology.