EurAsian Journal of BioSciences
Eurasia J Biosci 14, 3731-3739 (2020)

Particularities of the Internet-based virtual social environments within the context of information warfare

Gennadi B. Pronchev [1*], Aleksander P. Mikhailov [1], Aleksey P. Lyubimov [2,3], Andrey A. Solovyev [4,5,6]

[1] Keldysh Institute of Applied Mathematics, Moscow, RUSSIA
[2] Russian Academy of Sciences, Moscow, RUSSIA
[3] Diplomatic Academy of the Ministry of Foreign Affairs of Russia, Moscow, Russia, RUSSIA
[4] Moscow Pedagogical State University, Moscow, RUSSIA
[5] Kutafin Moscow State Law University, Moscow, RUSSIA
[6] Arbitration Court of Moscow Region, Moscow, RUSSIA
*Corresponding author: pronchev@rambler.ru

Abstract

The research deals with questions of information warfare in virtual social environments of the Internet. In the work, statutory and legal documents of the Russian Federation in the domain of information protection are analyzed. Particularities of the Internet-based virtual social environments are discussed: the popularity of virtual social environments among users, the existence of users' virtual identities, the network structure of information dissemination on the Internet, isotropy of virtual social environments, process capacities for manipulating users. The authors put forward the sociological substantiation for the mathematical model of information dissemination in virtual social environments having the network model of information dissemination; the conceptual description of the process is suggested. Although the state makes significant efforts at the legislative level for preventing the harmful information action on its citizens on the Internet, there is a number of particularities of virtual social environments which allow completing them only in part. The research findings can be of interest for specialists dealing with problems of information warfare and information security of virtual social environments.

Keywords: information warfare, virtual social environments, the Internet, mathematical modeling, isotropy of social environment, virtual identity, manipulations

Pronchev GB, Mikhailov AP, Lyubimov AP, Solovyev AA (2020) Particularities of the Internet-based virtual social environments within the context of information warfare. Eurasia J Biosci 14: 3731-3739.

INTRODUCTION

The development of social services of the global Internet network based on the modern information and communication technologies has promoted the emergence of academic networking, multimedia tools, metrics, online resources and new virtual social environments with preset properties (Pronchev, 2013; Pronchev, Proncheva & Goncharova, 2019; Soltovets, Chigisheva & Dmitrova, 2020; Strielkowski & Chigisheva, 2018; Zaitseva et al., 2020).

Internet-based virtual social environments have become convenient platforms for civic self-organization both in Russia and in other countries of the world (Pronchev et al., 2018). They "have an impact on the structure of public movements and individual citizens' communities rendering it more "horizontal" and free from intermediaries. It is often the case that individual teams get grouped around one or several leaders who coordinate their actions with leaders of other groups to achieve the common objective, creating a polycentric horizontal network. In other words, … can be used efficiently for creating and maintaining strong and centralized organizations" (Usacheva, 2012).

Regrettably, alongside new useful opportunities for virtual social environment users (Pronchev, & Muravyov, 2011; Goncharova et al., 2017), some negative consequences can be observed. So, slanderous information is posted in virtual social environments frequently, and messages sent to a user can be threatening, bullying, humiliating the user, or contain insulting, vulgar comments (Willard, 2003). Law-breakers can take advantage of a user's confidential information for criminal purposes (Korablev, Lontsov & Pronchev, 2010; Solovyev et al., 2020); it can also be played into for imposing goods and services (Azarian & Pronchev, 2016), and for manipulation in information

Received: October 2019
Accepted: April 2020
Printed: September 2020

wars (Mikhailov et al., 2018; Petrov et al., 2018). Social deviations are to be seen in virtual social environments increasingly more often (Vasenina, Kuleshova & Pronchev, 2018; Pronchev, 2020).

In this paper, the authors are going to analyze some particularities of the Internet-based virtual social environments that prevent information protection in them. An approach to mathematical modeling of information dissemination processes in virtual environments will also be suggested, taking into account the network model of information dissemination.

LITERATURE REVIEW

The tools, methods, and technologies of manipulative action during information warfare have long been under study both in Russia (Volkogonov, 1983; Osipov, 2000) and in other countries of the world (Schiller, 1973; Schiller, 1976). For reducing the negative impact, the state adopts legal regulation measures.

The legal bases of regulation are contained both in the Constitution of the RF (Constitution, 1993), and in a number of basic statutory instruments. Among the latter, the following should be listed: Federal law dated December 28, 2010 No. 390-FZ “On security” (FL, 2010), “The strategy of national security of the Russian Federation” approved by the Decree of the President of the Russian Federation dated 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 dated September 9, 2000 No. 646 (Decree, 2016), and other legal acts.

All the subsequent relevant enactments were aimed at elaborating and fulfilling the said documents (Lyubimov & Shchitov, 2017).

The Federal Service for Technical and Export Control defines “Security of information” as the “condition of the information being protected against internal or external threats when processed by computer engineering means or automated systems” (FSTEC, 1992).

As for detailing these issues, the governing and specifying documents are “Recommendations for standardization R 50.1.053-2005. Information technologies. Basic terms and definitions in scope of technical protection of information” (Gostinform, 2005) and GOST R 50922-2006 “Information protection. Detection, prevention, and liquidation of consequences computer attacks and computer incident response. Terms and definitions” (FSTEC, 2006) which imply ensuring confidentiality, accessibility, and integrity of information.

The doctrine of information security (Decree, 2016) supplements the said notions with social protection of national interests in the domain of information that are determined by the total of balanced interests of individuals, society, and the state (Lyubimov & Shchitov, 2018). Basically, all the above requirements are stipulated in many documents of the international importance.

When defining all levels of security, they can be worded as follows: national security, information security, and information protection which includes legal, organizational, technical, economic, moral and ethic framework of ensuring information security.

The following are referred to organizational and technical information protection methods (Novikov, Galushkin & Aksenov, 2017; Razumovskaya et al., 2018):

- possibilities of identification of technical devices and software constituting a hazard for the normal functioning of information and telecommunication systems; prevention of information getting intercepted via technical channels; the use of cryptographic information protection means during storage of the information (whenever available) and the use of other protection means;
- certification of information protection means, licensing of activities in the domain of the state secret protection, standardization of ways and means of information protection;
- enhanced law enforcement activity of the federal executive authorities and executive authorities of subjects of the Russian Federation, as well as prevention and repression of offences in the domain of information, detection, conviction, and prosecution of persons committing crimes in the said domain;
- the development, use, and improvement of information protection means and methods of controlling the efficiency of the said means; the development of protected telecommunication systems, enhanced reliability of specialized software;
- proactive creation of systems and means for preventing unauthorized access to the information being processed, special actions causing destruction, deletion, and distortion of the information, as well as changes in design functioning modes of systems and means of informatization and communication;
- monitoring of information security indicators and supervision of actions of the personnel in protected information systems; training of specialized workforce reserve in the domain of information security.

Organizational and technical methods of ensuring information security are logically supplemented by economic methods which include:

- the system of financing the provision of the state information security;

- creation of efficient financial instruments for implementing organizational and technical methods of ensuring information security, as well as of the required legal framework corresponding to this process; creation of the relevant insurance system for information risks of individuals and entities.

Legal support relies on adherence to the principles of legality and balancing the interests of citizens, organizations, and the state represented by its agencies; the state is the guarantor of overcoming possible conflicts and risks of various kinds.

The system of organizational information protection framework includes developing organizational and administrative documents and corporate regulatory acts; the list of such documents can number several scores according to the levels of protection of this information. This activity is performed on the basis of the effective legal acts, other statutory documents of the Russian Federation on ensuring information security, and the internal documents of the very organizations.

In general, it can be stated that the Russian Federation currently has all the necessary and sufficient organizational conditions for ensuring information protection at the federal and local levels.

METHODOLOGICAL FRAMEWORK

The objective of this research is studying the particularities of the Internet-based virtual social environments which objectively prevent information protection in information warfare.

The main tasks of the research are as follows:

1. Analyzing the statutory and legal documents of the Russian Federation in the domain of organizational issues of information protection.
2. Identifying the particularities of the Internet-based virtual social environments which objectively prevent information protection.
3. Analyzing the mechanisms of influence of the particularities of the Internet-based virtual social environments preventing information protection.
4. Developing the sociological substantiation for the mathematical model of information dissemination in virtual social environments, with the network model of information dissemination taken into account.

For achieving the tasks associated with analyzing the particularities of virtual social environments of the Internet that objectively prevent information protection in information warfare, the following research methods were used: the comparative and legal one, the systemic and structural one, and logical and semantic analysis.

The comparative and legal method was used for finding out the common and the different between the sources of law within the legal system of the RF as for the elements of information security.

The use of the systemic and structural method enabled the authors to explore and analyze in more detail the mutual influence of the Internet-based virtual social environments on information warfare.

The logical and semantic analysis was used for searching for the correct definitions.

In the work, secondary data of the results of the Russian and foreign sociological studies are used.

RESULTS AND DISCUSSIONS

Popularity of Virtual Social Environments

According to the Digital 2020 report (Wearesocial, 2020), presented by We Are Social and Hootsuite, it is 81% of the total population, or 118 million people, who have an access to the Internet in Russia. An average Russian is online for 7 hours 17 minutes every day, spending 2 hours 26 minutes in social networks. Russia’s most popular ones are WhatsApp, Viber, and Vkontakte. The audience of social networks amounts to 70 million people, or 48% of the total population of Russia (Wearesocial, 2020).

Virtual social environments of the Runet are the principal source of information for the greater part of the Russian young people; meanwhile, they are the most active Internet users, too. According to the results of the research “Social portrait of a contemporary Russian student” (Osipova et al., 2018), it has been found that “of all kinds of mass media, the vast majority of students (93,9%) prefer various Internet-based mass media (95,5% of younger bachelor degree students, 93,8% of senior bachelor degree students, and 91,1% of master degree students), while only just 4% opt for television (2,7% of younger 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 is preferred by a quite insignificant number of the questioned ones. In most cases, the Internet is used for communication (91,9% of the answers), searching for the required information (90,7% of the answers), entertainment (73,3% of the answers), studying (67,4% of the answers), working (43,1% of the answers), and gaming (11,5% of the answers) (Osipova et al., 2018).

Thus, as of today, Internet-based virtual social environments are the most popular means of learning the news for Russians. Most users do not strive verifying the received information against other sources – newspapers, television, and radio. As a consequence, false information in virtual social environments can be a serious information hazard for the people.

Virtual Identity

One of the important features of Internet-based virtual social environments is a “virtual identity”; it is created for each user and may considerably differ from the person’s actual identity (Korablev, Lontsov & Pronchev, 2010). This has been enabled by the fact that in social networks, people interact with each other not directly, but via data accounts (so-called profiles or accounts). A user account is an Internet page where the virtual social environment user places information, the confidential one included. Thus, the information “gets separated” from its initial carrier and starts living a life “of its own”. Meanwhile, it does not lose the association with the user’s identity, still remaining a description of the user’s social status, actions, and views. This association is very strong, because users can update details of their accounts at any moment.

While communicating in a virtual social environment with another user, one can stop perceiving the user as an actual identity and keep having an attitude to him or her as only an individual limited by this environment. Consequently, social norms get transformed in virtual social environments.

As for dissemination of misinformation in the virtual social environment, its key factor is the possibility of users supplying incomplete or distorted information. Thus, partial anonymity of social environment users is ensured. However, when users deem themselves physically inaccessible owing to anonymity, they get an illusion of impunity and permissiveness in their actions.

As an example, the story of a 38-year-old citizen of the town of Sovetsk, Kaliningrad region, can be cited. A criminal case was initiated against him under Article 319 of the Criminal Code of the RF. “The man commented on a message in a popular social network concerning the head of one of the region’s municipal units. Meanwhile, the citizen of Sovetsk did not mince any words all that much. It is not known exactly if it was a surprise for the unlucky commenter as some uniformed policemen came for him” (Orekhov, 2019).

Another characteristic feature of virtual social environments is the users’ “tolerance” to any changes of the information contained in the interlocutor’s account. It is assumed that the information initially specified there may be incomplete and inexact. This can be taken advantage of by law-breakers, too.

Network Structure of Information Dissemination: Sociological Prerequisites and Relevance of Building the Mathematical Model

According to the structure of information dissemination in the communicative environment, the hierarchical (**Fig. 1**) and network (**Fig. 2**) structure are distinguished (Osipova, Elishev & Pronchev, 2018). In the hierarchical structure case, information is disseminated from node to node.

For example, Ted 3 can receive some information from its initial source Jean 1 either via Ted 1, or via Olga 1. There is no direct transmission of the information from Jean 1 to Ted 3. Obviously, in both cases, the transmission of information can proceed by large time lags.

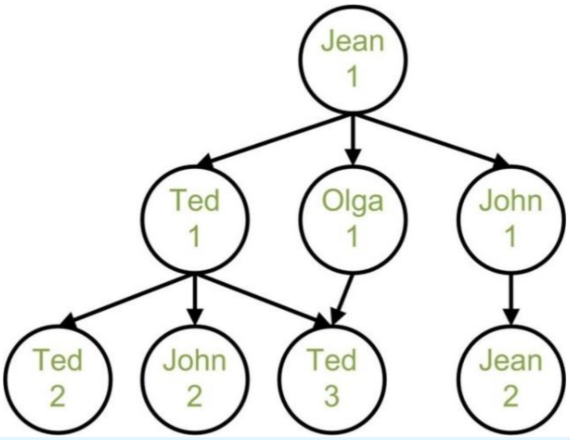

Fig. 1. Hierarchical information dissemination structure (Osipova, Elishev & Pronchev, 2018)

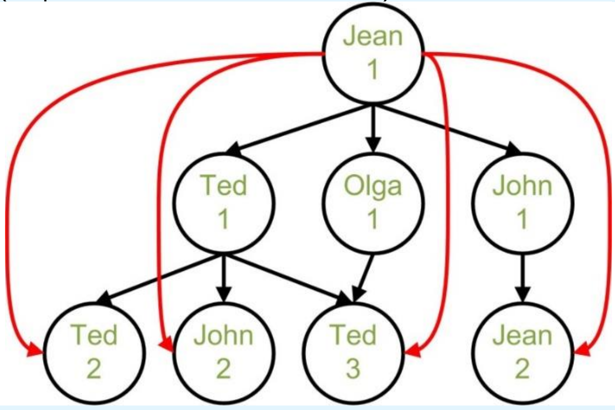

Fig. 2. Network information dissemination structure (Osipova, Elishev & Pronchev, 2018)

In the network structure case, information is disseminated to all recipients of the information simultaneously.

Clearly, in terms of information security, the second structure of information dissemination is more dangerous.

Should false information get disseminated, there can always be some people who will evaluate the incoming information critically. With the hierarchical model, such people can interrupt dissemination of the information down to “their” hierarchy, if necessary. Thus, they will delay ubiquitous dissemination of false information. Moreover, they can “launch” their own information disproving the received false information.

Meanwhile, given the network structure, the information will arrive to everyone at once. In this case, an irrelevant response can rapidly spread among the recipients. The people taking the information critically will not be able to influence this in any way already. So, mass hysteria may be triggered.

As an example, the case of false information spread about an emission of radioactive substances from the Leningrad Nuclear Power Plant can be given. The prosecutor of the town of Sosnovy Bor, where the LNPP is located, S. Rumyantsev noted (Davydov, 2008):

"About three days ago, half-joking messages were posted in the local Internet. Like, do not to take your kids for a walk, make sure you keep your windows, doors, and vent panes closed. Allegedly, somebody knew about the radioactive emission fact from a reliable source. But this is like a granny scribbled on the wall. And, probably, later on, this information was transmitted by other people, and its playful form was lost. As a result, all this has snowballed into the mass hysteria". During this time, the radiation background ranged within the norm in Sosnovy Bor. No surges in the town's radiation level were registered. Meanwhile, in Saint-Petersburg, they were buying out iodine at drugstores on a massive scale and panicking" (Davydov, 2008).

As the modern information and communication technologies develop, the Internet global network, in particular, it is the network structure of information dissemination that becomes the most relevant.

From the viewpoint of substantiating for the mathematical model of information dissemination in virtual social environments, the modeled process consists in a user of the network, hereinafter the seeder (from the verb to seed), making an entry (post) in a social network online (e.g., on Twitter, Facebook, or Vkontakte), and a number of other users (reposters) republishing this post (which is called reposting). The similar way of dissemination can be observed in jokes, joking photos and pictures, news of football and other topics, etc. If it is a political topic in question, a repost is most frequently an expression of political support. For example, a seeder (a well-known politician) voices a political reason or publishes lesser-known information, so his reposter makes a repost to bring this information to a greater number of people. With regard to this, reposters are distinguished between themselves according to their activity level (e.g., the most vibrant supporters of a certain politician can repost, say, half of his posts, while less active supporters can repost in one of a hundred cases or so). The mathematical model has to take into account these distinctions between the individuals. A promising theoretical basis for such a model seems to be the neurological model of decision-making by individuals under information warfare in the society (Petrov & Proncheva, 2019). It allows considering the said distinctions in an explicit form.

Notably, the similar network structure of information dissemination is carried out in the traditional mass media, too (radio, television). Anyway, when it comes to the Internet global network, information is also accessible to users in the case when a live stream is already over (i.e., in the offline mode). What is more, it is very difficult to completely remove this information from the public access. Even the "harsh" legal standards are of no help at times.

In 2016, the "right for oblivion" law became effective in Russia (FL, 2015). It has enabled users of the Internet to remove false or outdated information about themselves from the search results. However, from the total of 3600 addresses to the company from 1348 people, Yandex satisfied 27% only, rejecting 73%, among them 9% of partial rejection (their requests were met in relation of some links cited in the addresses) during the first six months of the law being in force (Rambler, 2019).

Social Isotropy

"The relations among users of social networks, if they are only considered as users, the remaining social qualities of these people apart, are the relations of equality: all of them are users of the network, all of them share with it a certain part of their personal data, and all of them get an access to some resources granted by its creators" (Pronchev & Muravyov, 2011).

The following case is illustrative. On May 10, 2009, one of the Livejournal users commented on an entry dedicated to the Great Patriotic War in the Internet-diary of D. A. Medvedev, the President of Russia, as follows: "All this is wonderful, but, say, in Krasnodar, veterans could not come to the Eternal Flame on the holiday. Its reconstruction has lasted for half a year already. Meanwhile, just a fortnight ago, two blocks away from the memorial, two multi-million projects were opened – the triumphal arc and the Saint Katherine complex. And there are almost no works conducted near the Eternal Flame – except that trees have been uprooted, and a bas-relief has been installed depicting Cossacks armed with the Kalashnikov guns for whatever reason. As a result, the citizens of Krasnodar laid floral tributes to the metal fence inclosing the Eternal Flame. It would be nice to hear your opinion of the situation" (Livejournal, 2009). On May 15, 2009, the President replied to this comment in person, posting the image of a sheet of paper with the comment text printout and a brief instruction handwritten under it: "Find it out. Punish the guilty. Report within three days" (Livejournal, 2009; Vesti, 2009).

The authors believe it was this case that has largely prompted the civil servants in Russia to open public reception rooms and direct-action feedback books in virtual social environments.

By replying to the comment of an ordinary Livejournal user, the President put himself in the conditions of a relative "vertical" equality with the user and in general with the citizens of Russia having an access to the Internet.

Thus, in the Internet-based social networks, unlike the "vertical" hierarchical structure, or "vertical" inequality (**Fig. 3**), all members of the community have the same "vertical" powers and authority, or "vertical" equality (**Fig. 4**).

Nevertheless, "horizontal" inequality may well exist against the background of "vertical" equality in the Internet-based social networks (see **Fig. 5**).

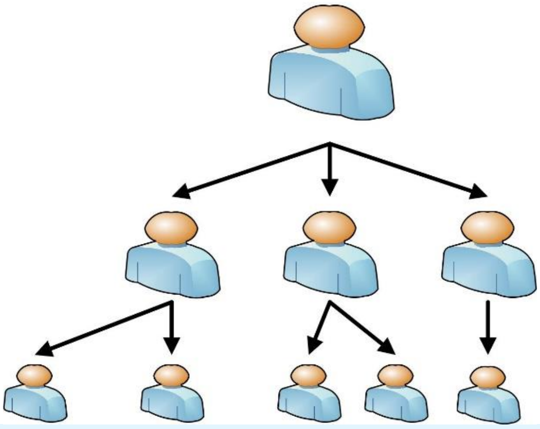

Fig. 3. “Vertical” inequality. The higher a tier in the hierarchy is, the more powers and authority it has (Pronchev, 2020)

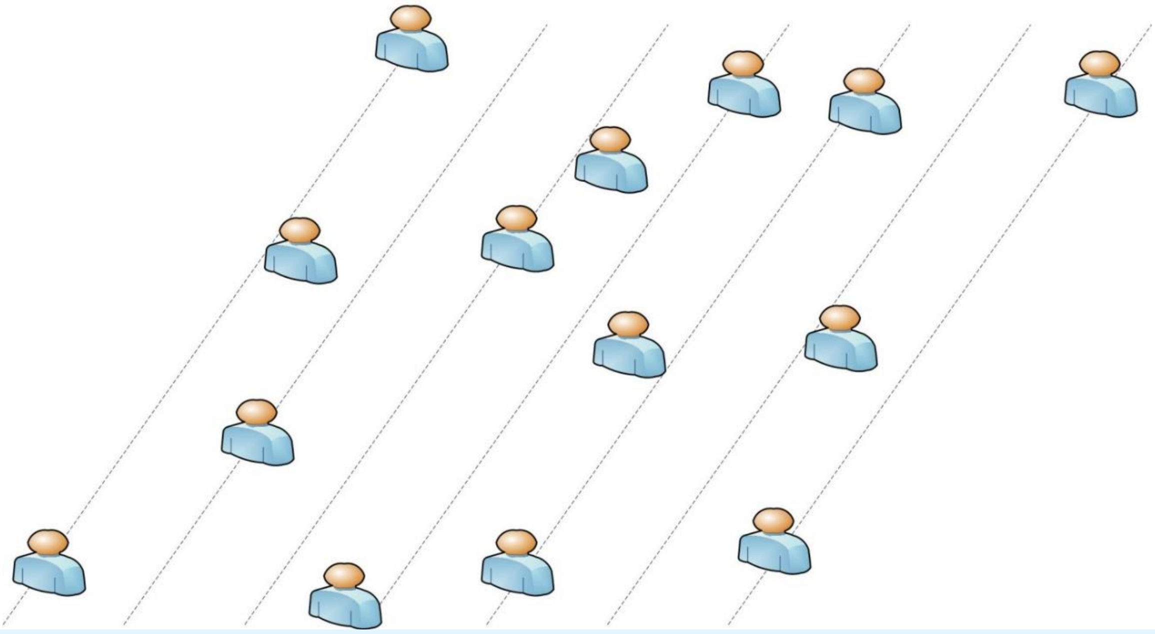

Fig. 4. “Vertical equality”. All members of the community have equal “vertical” powers and authority (Pronchev, 2020)

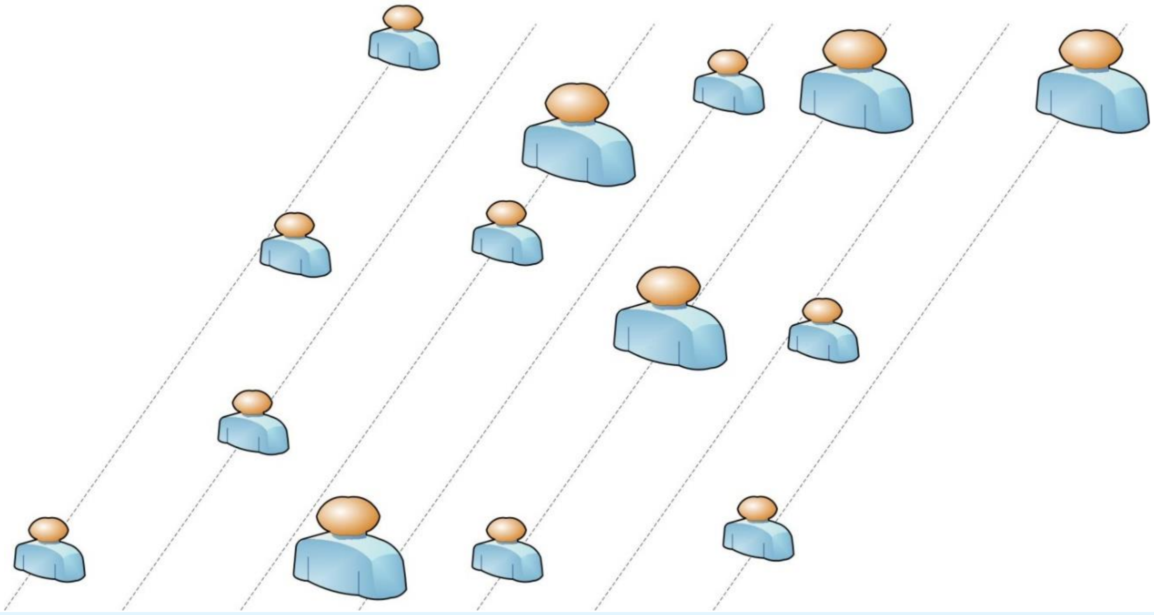

Fig. 5. “Horizontal” inequality. Members of the community have different “authority” (Pronchev, 2020)

In the case of “horizontal” inequality between the members of a community, it is the different “moral” authority of its members that has to be spoken about. For example, in the Internet community of fans of a football club, a former player of the club has a greater moral authority as a community member than an ordinary fan does. Nevertheless, his opinion is not the prevailing one from the point of view of acceptance by other members of the community.

By analogy to physics (Sivukhin, 1980), the situation when a community features both “vertical” and “horizontal” equality among its members can be called “isotropy of social environment”, and the very community – “isotropic social environment” (Pronchev, 2020).

Isotropic social environment promotes the emergence of social deviations. Really, in a social environment having neither powers, nor moral authorities, deviant behavior of members cannot be controlled. It is with this fact that frequent manifestation of verbal aggression in the Internet-based social networks is associated (Vasenina, Kuleshova & Pronchev, 2018).

Technological Manipulations

For a long time, the Western institutions proclaimed the Internet to be a symbol of freedom, openness, and publicity. However, at present, there is “legalized” censorship to be encountered in various segments of the Web (e.g. censorship in China), and elements of direct public opinion manipulation are observed, too. Trying to cater the interests of both the state and commercial structures, the largest Internet companies, such as Google and Facebook, create a unique virtual social environment for each person. The spyware used by them study the consumers in detail and feed special, biased information. As a result, users do not get a complete, objective picture of reality any more (Azarian & Pronchev, 2016).

Thus, the united information agenda gets split into local agendas (up to the individual ones). The approaches to mathematical modeling of this phenomenon are elaborated in the work by, A. Petrov and O. Proncheva (2020). It should be noted that their research does not take into account the network-related aspects of information dissemination, only presenting the society as an “integral environment”. Hence, the authors of this paper consider the integration of methods of taking into account the information agenda theory developed in the said work into the model emphasizing the network nature of information dissemination in virtual social environments to hold much promise.

On December 04, 2009, Google published the post “Personalized Search for everyone” in its corporate blog (Google, 2009). The Google PageRank algorithm which used to be operated in the Google search engine sorted the list of links in the hierarchical order: more respected websites were displayed higher than the others. The new Google algorithm introduced in 2009 personifies the search. So, it is not only the order in which links are displayed in search results that can differ but their number, too. Different content is displayed to different users.

Facebook enables advertisers to pick their audience according to location, sex, age, keywords, education, place of work, family status, and interests (Chernaya, 2018).

Thus, once anonymous, the virtual social environment turns into a tool for analyzing personal data and imposing certain information. What kind of resources will be accessible to users and what messages will be recommended depend on personalization. Therefore, the algorithms driving advertisement begin to govern people’s daily life, too.

CONCLUSION AND RECOMMENDATIONS

In recent years, Internet-based virtual social environments have become extremely popular with Russian users. For many, they are the principal source of information and a space to spend time in.

As a consequence, virtual social environments become a very attractive site for information warfare for many countries. Currently, Russia pays much attention to information protection at the legislative level. However, it is hindered by a number of particularities which are only inherent in virtual social environments on the Internet.

In the work, the influence of popularity of virtual social environments among users, particularities of users’ virtual identities, network structure of information dissemination on the Internet, isotropy of virtual social environments, and process capacities of manipulating users’ behavior have been analyzed. It has been demonstrated that the analyzed particularities are objective factors preventing information protection in information warfare. The authors suggest the sociological substantiation for the mathematical model of information dissemination in virtual social environments, with the network model of information dissemination considered; the conceptual description of the process is given that can serve as the basis for the mathematical model.

ACKNOWLEDGEMENTS

Studies developing the concept of virtual identity (Section 4.2), network aspects and approach to mathematical modeling (Section 4.3) and technological manipulations (Sections 4.5) were made by G.B. Pronchev and A.P. Mikhailov. In this part, the research was supported by the Russian Science Foundation (project № 20-11-20059 Mathematical models, game theory and empirical analysis in the study of informational warfare in society; Keldysh Institute of Applied Mathematics, RAS).

REFERENCES

Azarian DA, Pronchev GB (2016) Modern Internet technology and security of the person. Young scientist, 3: 61-63.

Chernaya A (2018) Targeting on Facebook: How to find your audience for advertising. Tricks you didn't know about. TexTerra. 25.06.2018. URL: https://texterra.ru/blog/targeting-v-facebook-kak-nakhodit-svoyu-auditoriyu-dlya-reklamy-priemy-o-kotorykh-vy-ne-znali.html

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

Davydov A (2008) Internet rumors led to mass hysteria. NTV.RU. URL: https://www.ntv.ru/novosti/132672

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

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

FL (2010) Federal Law No. 390-FZ of December 28, 2010 "On security". President of Russia. URL: http://www.kremlin.ru/acts/bank/32417

FL (2015) Federal Law of July 13, 2015 No. 264-FZ "On Amendments to the Federal Law "On Information, Information Technologies and on Information Protection" and Articles 29 and 402 of the "Civil Procedure Code of the Russian Federation". Rossiyskaya Gazeta - Federal Issue No. 154 (6725) of July 16, 2015. URL: https://rg.ru/2015/07/16/informacia-dok.html

FSTEC (1992) Protection against unauthorized access to information. Terms and definitions. Approved by the decision of the Chairman of the State Technical Commission of Russia on March 30, 1992. FSTEC Russia. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3

FSTEC (2006) GOST R 50922-2006. Information protection. Detection, prevention, and liquidation of consequences computer attacks and computer incident response. Terms and definitions. FSTEC Russia. URL: https://fstec.ru/component/attachments/download/2770

Goncharova IV, Pronchev GB, Monakhov DN, Vasenina IV, Zubova OG (2017) Remote Banking Services for the Visually Impaired in Britain as a Tool for Creating Barrier-Free Environment. Eurasian Journal of Analytical Chemistry, 12(7): 1405–1414.

Google (2009) Personalized Search for everyone. Google Blog. URL: https://googleblog.blogspot.com/2009/12/personalized-search-for-everyone.html

Gostinform (2005) Recommendations for standardization R 50.1.053-2005. Information technologies. Basic terms and definitions in scope of technical protection of information. Gostinform.ru. URL: https://gostinform.ru/normativnye-dokumenty-po-texnicheskomu-regulirovaniyu-i-metrologii/50-1-053-2005-obj43284.html

Korablev MN, Lontsov VV, Pronchev GB (2010) Protection of confidential information on social networks of the Internet. Sociology, 4: 33-45.

Livejournal (2009) Comment on Dmitry Medvedev's blog on the Livejournal.com to the video message "On the Great Patriotic War, historical truth and our memory". Livejournal.com. 07.05.2009. URL: http://community.livejournal.com/blog_medvedev/25564.html?thread=463-3308#t4633308

Lyubimov AP, Shchitov AN (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.

Lyubimov AP, Shchitov AN (2018) Modern scientific and technological priorities of the Russian Academy of Sciences. Representative power-XXI century, 7: 26-33.

Mikhailov AP, Petrov AP, Pronchev GB, Proncheva OG (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.

Novikov VK, Galushkin IB, Aksenov SV (2017) Information security and information protection. Organizational and legal basis. Edited by V. K. Novikov. Moscow: Hotline-Telecom.

Orekhov I (2019) For the Internet-chatter will have to answer. Komsomolskaya Pravda, 17.10.2019. URL: https://www.kp.ru/daily/27043.4/4108154

Osipov GV (2000) Social myth-making and social practice. Moscow: Norma.

Osipova NG, Elishev SO, Pronchev GB (2018) Mass information media and propaganda mouthpiece as a tool for manipulating and social inequality factor among the young people. Astra Salvensis, 6: 541–550.

Osipova NG, Sinykov AV, Elishev SO, Kanevsky PS, Trofimov SV (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, Mikhailov A, Pronchev G, Proncheva O (2018) Using search queries to analyze public attention to one-time political events. In: Proceedings of 2018 11th International Conference “Management of large-scale system development”. MLSD 2018, Art. 8551806. https://doi.org/10.1109/MLSD.2018.8551806.

Petrov A, Proncheva O (2019) Propaganda Battle with Two-Component Agenda. CEUR Workshop Proceedings, 2478: 28-38. URL: http://ceur-ws.org/Vol-2478

Petrov A, Proncheva O (2020) Modeling Position Selection by Individuals during Informational Warfare with a Two-Component Agenda. Mathematical Models and Computer Simulations, 12(2): 154-163.

Pronchev GB (2013) Remote access educational information system. In: Technology to build education systems with specified properties: Materials of III International scientific-practical conference, 12 – 13 November 2012. Moscow, 284-286.

Pronchev GB (2020) On the features of virtual social environments of the Internet that contribute to social deviations. Education and law, 3: 200-208.

Pronchev GB, Monakhov DN, Proncheva NG, Mikhailov AP (2018) Contemporary virtual social environments as a factor of social inequality emergence. Astra Salvensis, 6: 207-216.

Pronchev GB, Muravyov VI (2011) Social networks as a factor in Russia’s transition to innovative development. Sociology, 3: 36-56.

Pronchev GB, Proncheva NG, Goncharova IV (2019) Modern management of media environment: negative effects for the society of today. Journal of Environmental Treatment Techniques, 7(4): 836-840.

Rambler (2019) Google and Yandex almost do not comply with the law on the “right to oblivion”. Rambler.Ru. 15.03.2019. URL: https://news.rambler.ru/internet/41878242-google-i-yandex-pochti-ne-vypolnyayut-zakon-o-prave-na-zabvenie

Razumovskaya M, Zaitseva NA, Larionova AA, Chudnovskiy AD, Breusova EA (2018) Prospects for applying various forms of organizational integration to improve the quality of education. Astra Salvensis, 6: 348-362.

Schiller HI (1973) The Mind Managers. Boston: Beacon Press.

Schiller HI (1976) Communication and Cultural Domination. London: Routledge.

Sivukhin DV (1980) General course of physics. Moscow: Science.

Solovyev AA, Sheiafetdinova NA, Zavadskaya LN, Krainov VI, Kharlamov PV, Kovalev KS (2020) Internet and Personal Data as Factors of Influence on Legal Culture. Modern Law, 1: 16-22.

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.

Strielkowski W, Chigisheva O (2018) Research functionality and academic publishing: Gaming with altmetrics in the digital age. Economics and Sociology, 11(4): 306-316.

Usacheva OA (2012) Civil mobilization networks. Social Sciences and Contemporary World, 6: 35-42.

Vasenina IV, Kuleshova, NS, Pronchev GB (2018) Verbal aggression in virtual social environments. Astra Salvensis, 6: 29-37.

Vesti (2009) Vesti.net: officials learn blogs. Vesti.Ru. 25.11.2009. URL: http://www.vesti.ru/doc.html?id=327682

Volkogonov DA (1983) Psychological warfare: Subversive actions in regional societies. consciousnesses. Moscow. Voenizdat.

Wearesocial (2020) Digital 2020. URL: https://wearesocial.com/digital-2020

Willard N (2003) Off-campus, harmful online student speech. Journal of School Violence, 2(1): 65-93.

Zaitseva NA, Larionova AA, Shapovalov NI, Povorina EV, Takhumova OV, Zhukova MA, Dvornikova TA (2020) Regulatory aspects and problems of personnel certification taking into account the requirements of professional standards. International Journal of Psychosocial Rehabilitation, 24(03): 2179-2188.