MODESTUM
OPEN ACCESS

Eurasian Journal of Analytical Chemistry, 2018, 13(1b), em82
ISSN:1306-3057
Research Paper https://doi.org/10.29333/ejac/102247

An Attitude of Citizens to State Control Over the Internet Traffic

Roza Sh. Akhmadieva [1*], Larissa N. Ignatova [2], Galina I. Bolkina [2], Andrey A. Soloviev [3], David V. Gagloev [4], Maria V. Korotkova [5], Valentina I. Burenina [6]

[1] Kazan State University of Culture and Arts, Kazan, RUSSIA
[2] Plekhanov Russian University of Economics, Moscow, RUSSIA
[3] Moscow State Pedagogical University, Moscow, RUSSIA
[4] People's Friendship University of Russia (RUDN University), Moscow, RUSSIA
[5] Financial University under the Government of the Russian Federation, Moscow, RUSSIA
[6] Moscow State Technical University named after N.E. Bauman (National Research University), Moscow, RUSSIA

Received 14 August 2018 ▪ Revised 8 November 2018 ▪ Accepted 22 November 2018

ABSTRACT

The problem of using Internet resources is becoming increasingly urgent. A world-wide system of computers, local networks, servers, voluntarily joined together into one network distributed across the planet, which serves to exchange information, has been created, and the question of regulating this network arises. This is a big social problem, and for this reason it is so widely and hotly debated around the world. In this regard, the purpose of this article is to analyze the attitude of citizens towards the state control over Internet traffic in the 21st century. Research methods: The leading research method is a survey conducted with residents of a metropolis, which allows considering this problem as a dynamic process. Results of the study: The article presents the results of the interviews and shows that the majority of users of Internet resources have a negative attitude towards the control of user Internet traffic by the state. The majority of the population is not only not ready to pay the costs to communication companies, but is also ready to show civic activism in obstructing the functioning of the law. The respondents indicated the following main objectives, which the state adheres to, controlling the users' network traffic: preventing recruitment to prohibited terrorist organizations; prevention of acts of terrorism; drug trafficking prevention; receiving information about public opinion; prevention of illegal actions and rallies; receiving information about the activities of opposition parties; obtaining compromising materials. Practical significance: The data obtained in the work can be used in jurisprudence, practical psychology, as well as for further theoretical development of this issue.

Keywords: state control, legal regulation, Internet traffic

INTRODUCTION

Nowadays the Internet is a necessary part of modern people life. It is trivial to speak about its significance. But an issue of Internet control is a social problem and that's why it is so widely and hotly debated across all over the world. The Department of Connection and Communication offered to set state control of the Internet traffic in Russia. According to this offer it is possible to create systems of monitoring of the work of critical elements of the Runet infrastructure to make government agency understand device of the Russian Internet segment and so the could protect it from external attacks.

In particular, as "Statements" write, someone suggested to invite a registry of IP-addresses, that are issued by the Dutch company in automatic mode. The Runet will stop working minimum for a day, if the malfunction takes place, so that's why the department offers to create a copy of the registry of addresses. And there is one more

© 2018 by the authors; licensee Modestum Ltd., UK. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/).
✉ roza79.08@mail.ru **(*Correspondence)** ✉ Ignatova.LN@rea.ru ✉ Bolkina.GI@rea.ru
✉ sportlaw2014@rambler.ru ✉ david.vebber@yandex.ru ✉ Maria_979@mail.ru ✉ Bvi@bmstu.ru

suggestion to create the registry of exchange points for security. Such points are allowed to built reserve channels of connection for protected communications using the budget publications of "Statements".

The necessity of the registry IP-addresses (unique computer addresses in the net) is explained as nowadays all IP-addresses are issued by Dutch company RIPE NCC, operators always apply the database of this company and on this base they create traffic routes and all the Runet will fall, if the information of Russian IP-addressees disappears from the RIPE NCC registry. The government suggests creating a copy of the IP-addresses registry that will automatically check the availability of Russian addresses in the database. This service will be suggested to operators by the government, but it won't be necessarily to use it, member of "Statements"tells [1]. Based on this information the government suggests operators and internet-companies to build spare channels that will improve network connectivity, politician continues. According to him, the government doesn't have an aim to follow the content of transferred information, it could be done by operators.

It is simple to find a necessary information in the worldwide web nowadays, that is inaccessible and illegal in real world. You should only type the rights words in the search system and the user enters the real garden of the forbidden fruits: pictures for pedophile, instructions for making explosive, sale of drugs, Nazi slogans. These secrets and much more are open for everyone, falling into the Net [2-5]. According to Internet portal Vavilon, a number of persons, who actively use worldwide net, has increased from 16 million to 3.2 billion of people (from 0.39 to 43.4% of population of a planet). Number of users will reach 4.1 billion by 2020 year. It is about 60% of population. According to the engagement rating of using the Internet in European countries, Russian Federation takes 1st place: 17% of internet users lives in Russia. Germany takes 2nd place – 71.7 million people (11.4% of all European users). And Great Britain takes 3rd place, where 53.3 million people use the Internet, its 9.8% of Europeans [6].

Talking about service activities of law enforcement agencies and practical aspect of a struggle with crime, Russian MIA representative D.V. Chepchugov [7] signs that the crime is really exists in the Internet, although the Internet is know as virtual. Practice of law enforcement agencies, analysis of criminal cases show that there is a real threat of growth of offenses, related to the Internet [8-11].

First of all, it is a threat for the government and its infrastructure. There are certain examples of information war and technogenic terror. Variety of breaking persons' constitutional rights and interests, related to violation of the rights to inviolability of information, inviolability of private life, confidentiality of correspondence etc. The most dangerous threat is rapidly growing crime of e-commerce sphere. The level of virtual crimes increased every year [12-16].

Responsibility for electronic types of crimes of computer information is a novation of our criminal law. It first appeared in the new Criminal Code. It is a Chapter 28; Pages 137, 138 are devoted to protection of constitutional rights of citizens. Also the government sees a necessity to control all the Internet, it creates a censorship and analyses net traffic. The USE made the first step after terrorist acts on 11th of September, 2001 and created a project TIA – total information awareness. According this project, special services of American services could catch all information in the Internet, if it brings a danger for internet safety. Is it worth talking about "the cradle of democracy" - social resonance in the country, that was created due to these actions. Sensational case of Edward Snowden became an apogee of the USA government line. Everyone who even watches a bit of what's happening in the world heard about this case.

Some innovations were established in the sphere of state control of the Internet during last years, such as: Federal list of extremists' materials (written by the Minister of Russian justice, based on the decisions of courts and introduces bi the law "About counteraction of extremist activity" from 25th of July, 2002) was published on 14th of July, 2007.

Russian providers started block access to resources on this list since 2008, although there was no legal basis for such lock at that time. On 28th of July, 2012 the President of the Russian Federation Vladimir Vladimir Putin signed a law introducing the concept of extrajudicial blocking of websites ("On Amending the Federal Law" On Protection of Children from Information, causing harm to health and development "and certain legislative acts of the Russian Federation Federation"). According to this law, from November 1, 2012 there is a register of prohibited Internet resources in Russia. The blacklist initially hits sites, containing information about drugs, child pornography and appeals for suicide, and also resources for which a court decision was issued on violation of the law. Roscomnadzor is an operator of registry of malicious information. The Ministry of Internal Affairs, the Federal Service for the control over drug (FSCD) trafficking and Rospotrebnadzor may also take the decision to include sites in the "black list". Roskomnadzor, FSCD and Rospotrebnadzor developed a single list, which contains definitions of the terms "child pornography", "propaganda of suicide and drugs on the Internet" on 23rd of November 2013. It contains criteria for assessing information on Internet sites that are prohibited from being distributed in Russia.

On August 1, 2013, the so-called anti-piracy law joined the force in Russia ("On Amendments to Legislative Acts of The Russian Federation on the protection of intellectual property rights in the information-telecommunication networks ", was signed by the President of the Russian Federation Vladimir Vladimirovich Putin on July 2, 2013), who introduced the procedure of pre-trial blocking of sites with unlicensed films, serials.

Roskomnadzor carries out such blocking on the complaint of the right holders, whose application is considered by the Moscow Court. On February 1, 2014, a law came into effect that gives Roskomnadzor the right to o blacklist and block Internet resources with calls for extremism and riots by the request of the Prosecutor General or his deputies without a trial. On July 25, 2014, the order of the Ministry of Communications on April 16, 2014 came into force, March 31, 2015 lead SORM equipment to new performance criteria, which collects more detailed and accurate data about users of Internet-communications and storage of a complete record of their network interactions for a period of at least 12 hours. On August 1, 2014 so-called law on bloggers came into force the ("On making amendments to the Federal Law "On Information, Information Technologies and Protection" and certain legislative acts of the Russian Federation on ordering information exchange using information and communication technologies, telecommunication networks », signed by the President of the Russian Federation Vladimir Vladimirovich Putin on May 5, 2014). The law obliges authors of Internet resources with an audience of more than 3 thousand users register in Roskomnadzor per day.

The restrictions established in Russia for mass-media are applied to such owners of sites and authors of blogs. On January 15, 2015, the State Duma introduced a package of laws with proposals to strengthen control over Internet users. The authors propose to make additions in the law on pre-judicial blocking of sites, obliging Internet resources and hosting providers to store data about users within half a year after the end of their activity, and also notify Roskomnadzor of "the commencement of activities involving the dissemination of information and the organization of data exchange between users of the network". The FSB, the Ministry of Internal Affairs and Rosfinmonitoring participated in the work on a package of draft laws, and law enforcement agencies were the initiators. The purpose of the law is to identify and suppress the terrorist, as well as any other criminal activity at early stages. From May 1, 2015 Roskomnadzor will be able to block access to websites with illegal copies of books, music and programs on the basis of amendments to anti-piracy law ("On Amendments to the Federal Law" On Information, Information Technologies and Information Protection "and the Civil Procedure Code of the Russian Federation", signed by President Vladimir Putin on November 24, 2014). Access to the site can be blocked forever due to systematic violation of intellectual property rights. This measure will be applied if the rights holder twice wins a lawsuit against the same resource. The Moscow City Court will make a decision on permanent blocking, as before. After that, Roskomnadzor will notify the operator about the court's decision within 24 hours, the lock will also be applied during 24 hours [17]. The law on the state control over traffic, put forward at the beginning of 2016, is needed not to control, but to protect the Runet in the case of foreign influence, for example, disabling the DNS system, and the document does not impose financial burdens or obligations on traffic filtering, the employee of one of the operators explained. According to him, "the essence of the initiative is that the state intends to monitor the volume of traffic routing, which is dictated by economic considerations and considerations of information and national security." The need to preserve the security of the consciousness of citizens from virtual information attacks is growing [18–21].

Do you think that only the state has "eyes and ears" in your computer? The general picture will be smeared by the fact that simple, civilian services collect information about us. It is worth using the so-called "developer tools" in Google browsers or FireFox to see what the user is interested in for a number of organizations. When you try to access the resource xakep.ru, only two requests are addressed directly to the site, all the rest from the list - to third-party organizations that collect information about your interests, as a rule, in order to form the advertising most targeted to your needs [2,5,22,23,24].

Commercial corporations collect information about your interests. The United States is monitoring its citizens in order to prevent terrorist attacks. Does the government of our country have any relation to this trend? Russia is concerned about the control and legal regulation of the activities of the global network on its sovereign territory. On June 24, 2016, the State Duma adopted the so-called "antiterrorist package", a significant part of which is devoted to the Internet. According to the document, communication operators and "information dissemination organizers" should store all the transmitted information, records of telephone calls, and the content of SMS messages within half a year. They are also required to store information about the data transferred and to assist the FSB in decrypting all traffic for three years. The largest Russian Internet companies - Mail.ru and Yandex, as well as profile associations RAEK and ROCIT, and even the working group "Communications and IT" under the Government of Russia were against the new law. Law prescribes to communication operators and "information dissemination organizers" (they may be recognized as any sites, the register is maintained by Roskomnadzor) to store all data transmitted by users.

A representative of the Russian government O.V. Rykov, speaking about the legal regulation of the use of the Internet in Russia, notes that the main thing in this situation is to focus on modernizing the legislation, as well as law-enforcement practice in attitude to certain areas of Internet use in such a way that they did not violate the constitutional rights of citizens. He believes that the procedure for registering domain names is required, which provides for the suppression of attempts to seize domain names that coincide with trademarks. And also it is necessary to solve the issue with an electronic digital signature. By the way, this law is almost ready. Thirdly, in his

opinion, it is necessary to amend the Law "On Information, informatization and protection of information". Rykov argues that this legislative act is already ready and is in the government [7].

"Everyone has the right to privacy, personal and family secrets ..." (Part 1), "to the secret of correspondence, telephone conversations, postal, telegraphic and other communications", "restriction of this right is allowed only on the basis of a judicial decision" (Part 2). According to Article 24 of the Constitution, "the collection, storage, use and the dissemination of information about a person's private life without his consent is not allowed "(Part 1), as the legal documents of the Russian Federation read. Disputes about the legality of the being taken measures are still being continued, there is a struggle here in the mind of a citizen between the need for one's own security and the need for a sense of one's own freedom.

MATERIALS AND METHODS

Methods of the Research

The following methods were used during the research: the study of scientific and regulatory sources, stating psychological and pedagogical experiment, socio-psychological diagnosis: quiz, questioning, conversation, observation, testing, expert evaluation; mathematical, statistical methods and methods of computer data processing.

In the inhabitants of the metropolis the questionnaire included the following blocks:

1. Knowledge of residents on the draft law of the Ministry of communications about the state control over Internet traffic

Residents were offered information: "the Ministry proposes to create a state monitoring system "resource use global addressing and global identifiers of the Internet (DNS and IP addresses)". This system also needs to monitor critical infrastructure elements of the Russian Internet", and asked what they know about it.

2. What laws concerning the Internet are known to residents of the metropolis.

Residents were offered the following options:

- Law "On Protection of Children from Information Harmful to Their Health and Development"
- legislative act "On the issues of protection of intellectual rights in information and telecommunication networks"
- Law "On Information, Information Technologies and Information Protection"
- other

3. The ratio of residents to state control over Internet users.

Answers:

- Negative
- Positive
- neutral

4. Knowledge of the basic goals adopted by the state, controlling network traffic users

Residents were asked to name their choices for what the state has to introduce control over Internet users.

Experimental Research Base

An empirical study was conducted with residents of the Samara metropolis. The sample was 470 people of different ages.

Stages of research

The study of the problem was carried out in three stages:

Stage 1 - development of initial positions on the basis of theoretical analysis of literature on the research topic; finding the purpose, object, subject, research tasks; the development of a general concept of research, which includes methodological principles and a project for the development of a research tool.

Stage 2 - development of a research tool to identify the attitude of Samara to the state control over the Internet traffic.

Stage 3 - is empirical study of citizens to the state control of Internet traffic. A sample was formed, and empirical data were collected. Preliminary results were obtained. There are analysis and interpretation of the results.

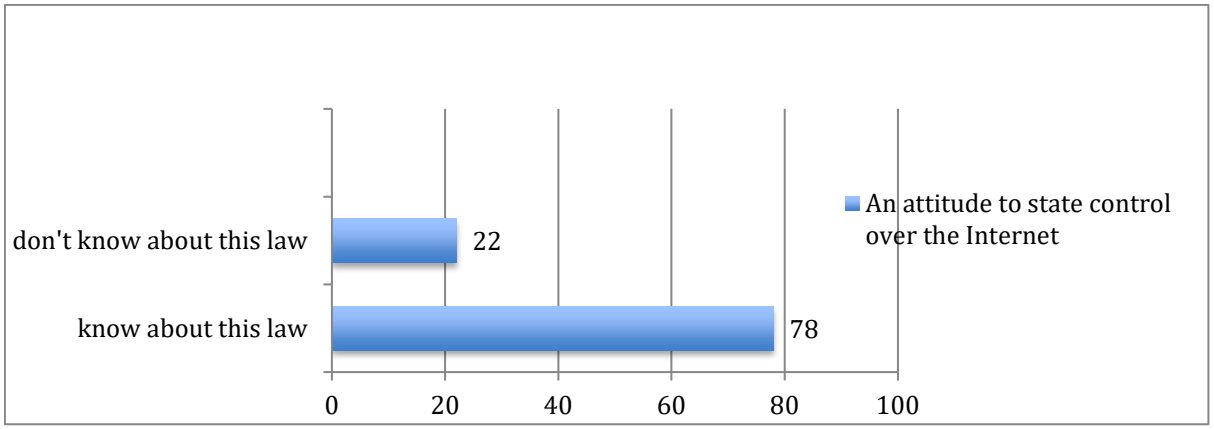

Figure 1. Knowledge of residents about the law

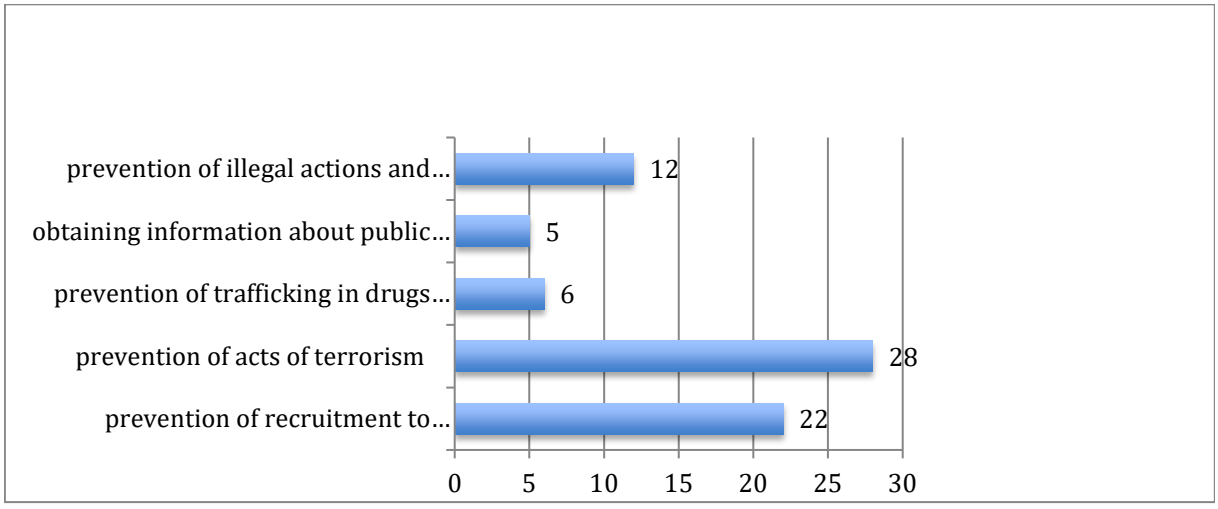

Figure 2. Objectives of state control over Internet traffic

RESULTS

On the base of our research, which was aimed at revealing the attitude of users to Internet monitoring, the following data were obtained: most users of Internet resources are negative about the control of user Internet traffic from the state (74%). About 12% of users have a neutral attitude. As for the positive attitude to Internet control, we can conclude that only 14% show this attitude. Consequently, the phenomenon of Internet monitoring is an actual problem because the majority of users refer to the policy of legalizing Internet control by the state negatively, even if this law has positive sides.

The following results were also obtained: the overwhelming majority of respondents showed the high level of awareness of this law. At the same time, almost 22% didn't hear this initiative (**Figure 1**).

In our opinion, laws of this magnitude should be brought to people without fail, because their consequences cause a huge response: the majority of the population is not only not ready to pay the costs to communication companies, but also is ready to show civic activity on obstruction of functioning of the law. The respondents indicated the following main goals, which are followed by State, when controlling the network traffic of users: prevention of recruitment to prohibited terrorist organizations (22%); prevention of acts of terrorism (28%); prevention of trafficking in drugs substances (6%); obtaining information about public opinion (5%); prevention of illegal actions and rallies (12%); obtaining information about the activities of opposition parties (14%); obtaining compromising materials (12%) (**Figure 2**).

The fight against terrorism is called one of the main reasons for the adoption of the law, but a negative evaluation of innovations and distrust of the state in its Internet policy make it possible to believe that personal rights and freedoms are placed above fear for security and stability, which speaks of the prevalence of universal humanistic values over attempts to create a hype around phenomena based on primitive fear. According to the newspaper The Guardian the results of research related to the control of user network traffic were received.

According to the research, illegible monitoring of the state for its citizens contributes to mistrust, conformism and mediocrity of society, the author points out, based on the data of numerous studies. The study of these evidences leads to a clear conclusion and warning: gathering information and mass surveillance is a serious risk to our mental health, productivity, social cohesion, and, ultimately, our future. Again, are we ready to make sacrifices for our own safety?

DISCUSSIONS

As early as 15 years ago studies have shown that surveillance leads to a high level of stress, fatigue and anxiety. It also reduces productivity and leads to a loss of personal control among employees in the workplace. A government that engages in mass surveillance can't claim that it values the well-being and productivity of its citizens. Secret tracking programs contribute to distrust between the state and the public. Studies have shown that people are tolerant of such programs only in exchange for guarantees of their own safety. But the moment comes when it becomes clear that people are sacrificing personal freedom, and this can lead to a split in society. And this behavior can lead to the fact that more than half of the population will cease to trust the state, which in turn will lead to the undermining of the democratic political system. The government can develop a false sense of absolute control, carrying out mass surveillance of citizens, without taking into account that this leads to a weakening of state power. According to The Guardian, the government clearly underestimates the psychological impact of such tracking programs on citizens. And it should be noted that the opinion of psychologists was not taken into account in the creation and development of these programs.

There are many theories of correlation between the social and the personal in sociology. Some researchers reduce the sum of the actions and opinions of individuals to the general picture of society, others suppose that the "whole" is not equal to its "parts". This discussion is also relevant for the issue that we are raising.

CONCLUSION

We note, turning to the estimates of the international human rights organization Freedom House, that Russia has presented a clear trend to strengthen control over the Internet society in recent years. It is also important to take into account that Russia is among the countries with partially free Internet.

Roskomnadzor include more than 45,700 online links (URL) into a single register of banned Internet-resources by the end of 2014. 64% of the resources are found in the propaganda and distribution of narcotic drugs, 15% in child pornography, and 12% in suicide. 317 people were entered in the register of blogger, although they expected to make 187.

According to a survey conducted by the Levada Center, more than half of the respondents citizens supported the introduction of censorship in the Internet because of the many dangerous sites, materials, one third of respondents considered the introduction of censorship on the Internet unacceptable, while more than a third of respondents would react calmly if the State Duma passed laws restricting Russians' access to the global Internet. Only 13% of respondents gave a negative answer to this question. The individual, of course, suffers from legislative practices. Does the group of individuals suffer damage? If society is reduced to a set of individuals, then it is obvious that yes. If society is something more, then more broad concepts come into play here - state security, for example. And we will be able to observe the results of the country's activities only some time after the examination of the consequences. But will not it be too late for reflection? Or will we regret not saying thank you for the care we need right away? Time will tell.

REFERENCES

1. The Guardian: "NSA and GCHQ: the flawed psychology of government mass surveillance". Retrieved from https://www.theguardian.com/science/head-sites/2013/aug/26/nsa-gchq-psychology-government-mass-surveillance
2. Alekseeva SI, Filippov TI, Witte SYu. On the issue of the circumstances of the implementation of the reform course S. Yu. Witte History of Russia: economics, politics, man. To the 80th birthday of Doctor of Historical Sciences, Professor, Academician of the Russian Academy of Sciences, B.V. Ananyitch. Proceedings of the Faculty of History of St. Petersburg State Universityю 2011;5:13-19.
3. Voyskunsky AE. Internet Studies in Psychology. Internet and Russian Society, Moscow: Gandalf; 2002.
4. Kramarenko MI, With N. Teen caught "in the network". Grapes. 2010;36:42-53.
5. Hartmann N. Ethics. St. Petersburg: Peter; 2005.
6. Yadov VA. Psychological research: methodology, program, methods. Samara: Samara University; 1995.
7. Rykov OV, Chepchugov DV. On the Legal Regulation of the Use of the Internet in Russia. Information Society. 2000;4:46-51.

8. Fichte IG. Compositions. St. Petersburg: Publishing House "Nauka; 2008.
9. Hjell L, Ziegler D. Theories of personality. St. Petersburg: Peter; 1997.
10. The Federal Law. "On Amendments to the Federal Law" On counteracting terrorism "and certain legislative acts of the Russian Federation in part of the establishment of additional counter-terrorism measures and public security"; 2016.
11. Scheler M. Formalism in Ethics and the Material Ethics of Values. Anthology of Realistic Phenomenology. 2006;2:56-79.
12. Krylov AN. Intrenet-journalism and virtual identity: selected aspects of the psychological portrait of a consumer of mass media Public relations and advertising: theory and practice. Pedagogical workshop "Creative in the profession." Theses of reports. Chelyabinsk: Center for Advertising Technologies; 2012.
13. Silaeva VL. The substitution of reality as a sociocultural mechanism of the virtualization of society. Moscow: MSTU; 2004.
14. Kondratiev I. Technology is virtual, the result is real. Computer world. 1997;35:7–13.
15. Mikhailov VA. Features of the development of information and communication environment of modern society. Collection of scientific papers "Actual problems of the theory of communication." St. Petersburg. Publishing house SPbGPU; 2004.
16. The Constitution of the Russian Federation. Retreived from http://www.constitution.ru/ Electronic resource "24 World": https://mir24.tv/news/13900589
17. Montesquieu Sh. On the spirit of laws or the relationship in which laws must to be in the arrangement of every government, morals, climate, religion, trade. St. Petersburg: publishing house LF Panteleeva; 1900.
18. Cherdymova EI, Sorokina TM. Organizational and psychological support for the formation of eco-professional consciousness of students. Samara: Samara University Publishing House; 2013.
19. Verchenov LN, Efremenko DV, Tishchenko VI. Social Networks and Virtual Network Communities. Moscow: INION RAS; 2013.
20. Goroshko EI. Communicative space of the Internet as an object of socio-cultural analysis. Odesky National Bulletin of the National University. 2010;15:130-136.
21. Luchinkina AI. Human psychology on the Internet. Moscow: Information Systems LLC; 2012.
22. Zakharova LG Great reforms of the 1860s-1870s: the turning point of the Russian stories? National history. 2005;2:151-168.
23. Filippova TV. The Internet as a tool for sociological research. Sociological Studies. 2002;9:115-122.
24. Goryavsky Yu. Back to the Future. World of Internet. 2001;21:55-61.

http://www.eurasianjournals.com