International Review of Management and Marketing

ISSN: 2146-4405

available at http: www.econjournals.com

International Review of Management and Marketing, 2015, 5(Special Issue) 160-169.

Special Issue for "Media as the Tool: Management of Social Processes"

Media as an Environment of Treats: 15 Years in the Shadow of the Information Security Doctrine

Iosif Dzyaloshinskiy[1]*, Marina Dzyaloshinskaya[2]

[1]National Research University Higher School of Economics, 20 Myasnitskaya Ulitsa, Moscow 101000, Russia, [2]Academy of Labor and Social Relations, 90, Lobachevsky Ulitsa, Moscow, 119454, Russia. *Email: imd2000@yandex.ru

ABSTRACT

This paper presents the results of research devoted to study of the Russians' attitude to media threats and the ways to minimize the damage caused by them. It is demonstrated that the number of peculiarities of the modern media that are recognized by different publics as threats is significantly less than the register offered by experts and the list of threats provided in the information security doctrine. The weight of evidence suggests that after 15 years of realization of the information security doctrine in a particular country, Russia will again have to return to understanding of the media threats as a global phenomenon requiring the same number of global solutions. And these solutions should be based on not only and rather than prohibitions and punishments but on development of the society of knowledge founded on the humanistic values and four fundamental principles reflected in the UNESCO Constitution: Promotion of freedom of expression in traditional and new media including the Internet; availability of quality education for everyone; respect to cultural and language diversity; universal access to information and knowledge, in particular, to the information being a public domain.

Keywords: Media, Media Threats, Media Security, Information Security Doctrine
JEL Classifications: O32, O33, O38, Z13

1. INTRODUCTION

With emersion of the Internet interaction of people with the media environment has sharply changed. Nowadays one can hardly imagine the human society, activity of mass media, education, political life, scientific research and entertainments without the Internet technologies. And as any global phenomenon significantly influencing development of the human society the Internet has its advantages and disadvantages.

The advantages usually include:

- Promptness in obtaining any information - the Internet user does not have to go to the library and look for necessary material, he/she can just open any browser and specify its condition in a search bar and choose the necessary one from the options offered;
- Information content - one can find several points of view for any topic offered and compare them and, thus, obtain the complete information;
- Technological effectiveness - use of the latest developments in the field of information and telecommunication technologies;
- Creativity - the user can use in his/her work best practices offered for free access in the Internet network and can on the basis of the information offered provide something of his/her own not similar to previous creations and, thus, express himself/herself;
- Extension of communication boundaries (social services and forums, e-mail) - ability to communicate, share experience, knowledge;
- Building of information competence including skills of work with the information (find, obtain, analyze, systematize, and use);
- Ability of on-going self-education and realization of personal potential.

But the scale of modern media and the processes taken place in this system begin to give rise to concern of many analytics and public figures (Information and psychological security in the mass

media, 2002; Pozdnyakov, 1994; Problems of information and psychological security 1996; UNECE Strategy for Education for Sustainable Development, 2005). In the most of these papers the primary emphasis is placed on the threats faced by the federal and corporate information and telecommunication systems. From this - technocratic - point of view the main objects ensuring information security are:

- Information resources containing data classified as the National Security Information and confidential information;
- Information means and systems (computer aids, data computing complexes, networks and systems), software (operating systems, data base management systems, other system and applied software), computer-aided control systems, communication and data transfer systems receiving, processing, storing and transmitting restricted information, their informational physical fields;
- Technical means and systems operating with public information but located within the facilities where restricted information is processed as well as the facilities designed for processing of such information;
- Facilities designed for holding private negotiations as well as negotiations, in the course of which the restricted data are communicated.
- The supporters of this point of view emphasize the following types of threats in this field:
- Activity of special services of foreign countries, criminal associations, organizations and groups, illegal activities of some individuals aimed at obtaining unauthorized access to information and ability to control functions of information and telecommunication systems;
- Use of imported firmware necessitated by objective lagging of domestic industry during creation and development of information and telecommunication systems;
- Violation of the established procedure of information acquisition, processing and transfer, intentional actions and failures of the personnel of information and telecommunication systems, equipment failures and software breakdowns within information and telecommunication systems;
- Use of information and communication means and systems not certified in accordance with the security requirements as well as means of information security and the efficiency of their control;
- Involvement of organizations and companies not having state licenses for execution of such types of activities for carrying out of works on creation, development and securing of information and telecommunication systems.
- The following is proposed as means, the use of which should ensure information security in accordance with this understanding:
- Prevention of information capturing from the facilities and objects as well as capturing of information transmitted through communication channels with the help of technical means;
- Elimination of unauthorized access to the information processed or stored in the technical means;
- Prevention of information leakage through technical channels occurred when using technical means for its processing, storage and transfer;
- Blocking of special hardware-in-the-loop impacts causing disruption, destruction, distortion of information or failures in operation of information means;
- Provision of information security when connecting federal information and telecommunication systems to external information systems including international ones;
- Provision of security of the confidential information during interaction of information and telecommunication systems of different protection classes;
- Detection of electronic eavesdropping devices installed in the facilities and technical means.

The main organizational and technical measures on ensuring of information security in the federal information and telecommunication systems include:

- Licensing of activities of the organizations in the field of information security;
- Certification of information facilities on compliance with the requirements of information security provision when carrying out works connected with the use of data being the National Security Information;
- Certification of the means on information security provision and control over efficiency of their use as well as the level of information protection against leakage through technical channels of information and communication systems and means;
- Introduction of territorial, frequency, energy, space and time limits in the modes of use of technical means subject to protection;
- Creation and application of the sheltered information and automated control systems.

The other approach - social and psychological - is demonstrated in the papers of the authors who, as a rule, base their reasoning on the provisions that the information security should be considered as a state of protection of an individual, different social groups and associations of people from impacts able against their will and wish to change psychic state and psychological characteristics of a person, modify his/her behavior and limit the freedom of choice (Shestoperov and Todorov, *2015*, Declaration on the Environment and Development; 1992; Doctrine of Information Security 2015; Johannesburg Declaration on Sustainable Development, 2002; Roshchin and Sosnin, 1995; Sakhalin Declaration "Internet and Socio-Cultural Transformations, 2015; Pilgun, Gradoselskaya, 2015; Federal Law of the Russian Federation dated December 29 2010).

The supporters of this approach emphasize such threats as:

1.1 Increase of Importance of Communicative Activity in Comparison with the Other Types of Activity

Communication becomes the main strategic game, in which success or non-success of a definite person, organization, social group and society in general (communication imperatives) is defined. Nowadays the weakest is not the person who cannot loudly declare himself/herself but the one who is absent in the communicative sphere - who is practically non-existent. Self-actualization of an individual is considered to be its external self-presentation.

1.2 Increase of an Individual's and Society's Dependence on Communication Networks and Processes

Absence of possibility to tap into communication channels (or disconnection from them) makes the person helpless. Communicative skills become the main qualification criteria of professional success. To ensure communication success it is necessary to constantly track the situation at the profile market and quickly react to dynamics of discussion environment.

1.3 Inability to Tell Theatricalizing from Reality. Substitution of "Real Reality" with "Virtual One"

Modern communication society exists in the world of artificially created images. They become that the people is considered to be the reality and serve as the guideposts for their thoughts, points of view, feelings and deeds. As the signs referring to real reality are substituted by so-called simulacra that referencing to themselves or other simulacra the people become even more beneted with communications that prevent them from accessing the real life existing outside this network. The person gets so closely beneted with communication that he/she is not able to see the loss of reality that is the real world is absolutely substituted with the virtual one and the person does not feel alienated from himself/herself and his/her fellow humans.

1.4 Inflation Processes in the Field of Communication (Devaluation of the Word)

Amount of communication increases similarly to the mechanism of money supply increase in the economics but during this the common understanding is even rarely achieved similarly to the situation when during money inflation even fewer goods can be bought for the same amount of money. As a consequence - belief in communication falls, the words, calls and mottos devalue.

Optimization of communication following the criterion of "mass character" leads to simplification of content and entertaining nature of the form. Mass media offering serious, complete information on events of local, national and global scale become even less of demand. Publications, TV-channels aiming to comply with the quick tempo of our time and support "clipping consciousness" of their audience get off. They present the material brassily, lapidary and in an easily "digestible" form. Absence of necessity to think, do definite intellectual efforts leads to atrophy, regression of "gray cells."

1.5 Increase of "deprivatization"

Information about a personality is considered as economically profitable goods and the source of power and the modern technological solutions provide novel possibilities for accumulation and use of such information and its turning into tools of social control and manipulating of the person's behavior. The most massed and everyday threat is creation of computer systems for capturing and processing of personal data. Modern computer technologies allow immediately exchange information, compare and converge personal data accumulated in different information systems.

The main official document, in the frameworks of which an attempt to combine these both approaches was taken, is the Information Security Doctrine approved by the Order of the President of Russia in September, 2000. In accordance with this document the Information Security of the Russian Federation is a state of protection of its national interests in the information field that is defined by the whole of balanced interests of a person, society and state (Grachev, 1998). In due course issue of the Order raised quite animated discussion connected with ambiguity of some provisions of the Doctrine. And though the discussion gradually faded the time passed showed that the problems remained. Moreover, new hazards emerged in the field of communication and information. Special attention is drawn to information security of children.

In accordance with the Russian legislation (Grachev and Melnik, 1996) the information security of children is a state of children's protection, in which the risk connected with doing harm to their health, physical, psychic, spiritual and moral development by the information including the one distributed through the Internet, is absent. The following information is considered to be forbidden for distribution among the children:

- Inducing children to doing actions threating their lives and (or) health including that inducing to doing harm to their health, committing suicide;
- Able to raise in children wish to take drugs, psychotropic and (or) intoxicating substances, tobacco products, alcohol and alcohol-containing products, beer and its derivatives, participate in gambling, prostitute, do vagrancy or beggary;
- Proving or justifying admissibility of violence and (or) savagery or inducing doing violent actions for people or animals except for cases provided by this Federal Law;
- Denying family values and forming disrespect to parents and (or) other members of the family;
- Justifying illegal behavior;
- Containing strong language;
- Containing information of pornographic nature.

Different materials (texts, pictures, audio, video films, music, images, links to external sources) containing violence, aggression, erotic and pornography, strong language, information spreading racial hatred, advocacy of anorexia and bulimia, suicide, gambling, drugs, etc. are included in the definition of problematic or "hazardous" content.

"Hazardous" content is a reason of the following problems:

- Children involuntary deal with such materials during rather "harmless" sessions in the Internet;
- Young users are often quite competent to find and get access to forbidden (by parents or law) content;
- Voluntary or involuntary watch of such materials negatively impacts children's psychic, behavior.

But the practice showed that the efficiency of activity on provision of security of both children and the citizens from so-called harmful information is rather low. And there is a necessity to return to analysis of both the threats and ways of protection from them or just minimize their harmful impact.

2. METHODS OF STUDY

An advanced study was conducted from May to July, 2015 to obtain necessary data.

At the first stage focus-groups were arranged with involvement of researchers of modern media. The experts were offered to formulate in free form main threats causing uncontrolled development of media and possible ways to minimize the damage caused. Summary of the responses obtained is provided below.

Then the polling survey of different categories of the citizens of Russia following a standardized questionnaire was conducted and the respondents were asked to express their attitude to the specified threats and ways to minimize damage in such questionnaires. Characteristics of the participants of this polling survey are presented in Tables 1-3.

The polling survey was conducted in 10 cities representing all the Federal Districts of Russia expect for the Crimea. The Crimean Federal District was not included in the number of territories under study as in this region the media situation significantly differed from the All-Russian up to the present time therefore the responses of the citizens of this district to a questionnaire cannot be considered representational for analysis of attitudes to the problems of the Russian media environment. Distribution of the respondents over the cities is presented in Table 4.

The results of the questionnaire held are given in percent from number of the respondents. Total amount of percent can be lower than 100% due to the fact that the options "other" and "no response" were excluded from the analysis due to paucity and they also can be higher than 100% in cases the question provided for possibility of more than one response.

Besides, an index of acceptance - a design value allowing obtaining an averaged value of level of the respondents' acceptance of one or another media threat - was used in the statistical data (calculation of the index of acceptance is given in Table 5). This index allows carrying out a definite comparison of attitudes to media threats of the respondents who differ in their gender, age, status and other characteristics provided in a fact sheet. Maximum value of the index of acceptance is 5.

Table 1: General characteristics of the respondents

Sex	
Male	23.4
Female	76.6
Age	
Under the age of 21	52.1
22-34 years old	26.3
35-55 years old	15.0
Over the age of 55	6.6
Education	
Secondary, vocational secondary education	6.6
Higher (incomplete higher) Journalism education	29.3
Higher (incomplete higher) Liber Arts education	34.7
Higher (incomplete higher) Technical education	13.8
Have academic degree	18.0
Field of work	
Material production (industry, agriculture)	3.6
Service industry (trade, public catering, housing and utilities infrastructure, public services, healthcare, social security)	9.6
Education	25.1
Culture/art	9.6
Mediation and consulting (including crediting, finances and banking business)	3.6
Regulatory and administrative authorities	1.2
Social organizations	3.1
Mass media	14.2
Students of the higher and secondary educational establishments	24.6
Temporarily unemployed, housewives, persons on care leave, etc.	5.4
Job title (% to the number of employed)	
Senior Management (Director, Deputy Director, Chief Engineer, Chief Specialist, Chief Editor, etc.)	14.8
Mid-level Management (Production Foreman, Department/ Business Unit Manager, Works Foreman, Group Leader, etc.)	19.6
Frontline Worker (Worker, Clerk, Creative Employee)	65.6

Table 2: Characteristic of the respondents' interaction with the internet

Frequency of the internet use	
Every day	84.4
As necessary	15.6
Duration of the time spent in the internet per day	
1-3 h	25.1
4-6 h	47.9
7-9 h	10.4
Over 10 h	16.1
Purpose of the internet use	
Search for information necessary for study/work	81.4
Communicate with friends in the social networks, blogs	71.9
Read news	68.3
Download films or watch them online	53.3
Download music, songs or listen to them online	49.1
Read books, newspapers, magazines	44.3
Pay for mobile connection, buy tickets, make bank transactions, etc.	32.3
Do shopping in the Internet-shops	25.2
Watch TV-programs	16.8
Use the Internet as a means of income	15.6
Look through horoscopes, dream-books, weather forecasts	15.0
Use services of state services	13.8
Download games or play online	10.2
Listen to radio	10.2
Visit dating sites	1.2

Table 3: Level of competence (knowledge, abilities, skills) of the respondents in modern communication spheres (average scores through the whole array; maximum value is 5 scores)

Competence level	Scores
Use of the possibilities of browser Internet-services, correct setting of search requests	4.5
Use of modern technical and mobile communication means	4.3
Critical perception of information, content placed at different Internet resources	4.2
Use of network communication	4.2
Necessity to take into account boundaries of privacy in the Internet and protect your private data	4.1
Use of digital and media services	3.9

Table 4: Distribution of the respondents over the cities where the polling survey was held

City	% to the number of the respondents
Moscow, the Central Federal District	14.8
Saint Petersburg, the Northwestern Federal District	13.4
Kazan, the Volga Federal District	12.8
Chelyabinsk, the Ural Federal District	12.1
Khabarovsk, the Far Eastern Federal District	9.4
Novosibirsk, the Siberian Federal District	9.4
Yekaterinburg, the Ural Federal District	8.7
Rostov-on-Don, the Southern Federal District	8.1
Nizhny Novgorod, the Volga Federal District	6.7
Pyatigorsk, the North-Caucasian Federal District	5.3

Table 5: Calculation of the index of acceptance

Level of acceptance	Coefficient
Absolutely agree	5
Rather agree	4
Have doubts	3
Rather disagree	2
Absolutely disagree	1

Step 1: Each level of acceptance given in the Table 5 is assigned with a definite coefficient:

Step 2: The number of the respondents agreed with a definite attitude on each media threat is multiplied by a definite coefficient and the product obtained is recorded in an appropriate column (at the intersection of media threat and level of acceptance).

Step 3: All the products obtained are summed up and the sum is recorded in each line (media threat).

Step 4: The number of the respondents expressed different level of acceptance are summed up on every media threat.

Step 5: The sum from Step 3: is divided by the sum from Step 4: This will be the index of acceptance.

Example

Step 2 and Step 3

No	27
Media threats	Modern media damage psychic of the people, form feeling of fear and despair
Absolutely agree	10 people×5=50
Rather agree	20 people×4=80
Have doubts	30 people×3=90
Rather disagree	40 people×2=80
Absolutely disagree	50 people×1=50
SUM 1	350

Step 4

No	27
Media threats	Modern media damage psychic of the people, form feeling of fear and despair
Absolutely agree	10 people
Rather agree	20 people
Have doubts	30 people
Rather disagree	40 people
Absolutely disagree	50 people
SUM 2	150

Step 5

No	27
Media threats	Modern media damage psychic of the people, form feeling of fear and despair
SUM 1	350
SUM 2	150
Index of acceptance	2.3 (350: 150)

3. RESULTS OF STUDY

3.1. The Media Threats: Main and Secondary

33 media threats formulated on the basis of the experts' survey were included in the questionnaire offered for respondents.

1. Activity in the cyber world does not promote civil activity in the real world; virtualization of political activity of the citizens rather hinders civil activity and conscious participation of the Russian citizens in the political process
2. In the communities of social networks in the Internet so-called "trolls" who are the users distributing distorted, incorrect but profitable for one or the other lobbyists information started to work for hire
3. Web-sites with such deviant information as concerning sexual relationships, scandals, destructive social actions, etc. prevail in the Internet
4. Information and communication inequality among the regions increases in Russia
5. Information and communication inequality among social groups and individuals increases in Russia
6. In the modern world media addiction has become a real threat to integrity, social adequacy of a person
7. Even more information is presented in the form of visual images in the modern media (traditional and new ones)
8. Even more people feel psychologically addicted to processes taken place in the media environment
9. Intrusion upon one's private life can be considered to be a significant ethic problem of modern media
10. Execution of modern common performance project often creates just illusion of that the participation in the communities of social networks in the Internet promotes forming and development of civil society
11. Life success of a modern person is to a large extent defined by the number and quality of his/her presence/representation in the Internet
12. Life success of a modern person is defined not with his/her skills but with the volume and quality of the information available to him/her
13. Information about a personality is considered as economically profitable goods and the source of power
14. People get even more inlined with comprehensive and quick-operating communication network having even fewer possibilities to influence the volume of information circulating inside it, quick-operation tempo or control them
15. Mass distribution of the Internet leads to an increase of cybercrimes: Illegal acquisition and use of information; unauthorized access to information resources; manipulating with information; illegal copying of data in the information systems, etc.

16. Uncontrolled access to information is dangerous
17. Abundance of different information disguises essential inaccessibility, closed nature of many segments of media environment
18. Image presentation of information in media maintains mythological way of thinking (figural interpretation of processes and phenomena not providing for understanding of their essence, real possible connections and dependences)
19. Dependence of social institutes on mass media increases
20. Mass media is guilty in blocking and poisoning of the children's and teenager's minds
21. Mass media can be accused of breaking moral principles
22. Mass media impose upon people unreliable order of the day, create illusory worldview
23. Mass media promotes incitement of social aggression and intolerance, forming "the image of an enemy"
24. Mass media form aiming at realization of unreliable life scenarios by the people
25. Modern media environment promotes breaking of traditional culture and aggravates systematic social and cultural crisis in Russia
26. Modern media create and impose upon people stereotype images (idols and reprobates)
27. Modern media damage psychic of the people, form feeling of fear and despair
28. Modern technological solutions provide novel possibilities for turning the information about a person into a tool of social control and manipulating of the person's behavior
29. Modern Internet supports the users' wish to obtain through its services information, distribution of which is limited by the rules of morality and laws in the traditional mass media
30. Social networks divide the users into interest groups, thus there is not a single communication environment in the Internet
31. Significant difference in the computer competence and possibilities to use modern information technologies increase psychological generation gap
32. There is a threat of deluge of information that is an uncontrolled increase of the amount of information making almost useless all the efforts to control information processes
33. Global media order has formed and within it the limited range of transnational corporations is the main subjects participating in the production of content and control of information processes.

The first and rather surprising result of the study is that the hierarchy of threats built in follow-up of the polling survey held does not coincide with those threats defined as the most important in the official documents.

Thus, the following were specified as the main media threats by the participants of the polling survey:

- Cybercrimes. (Mass distribution of the Internet leads to an increase of cybercrimes: Illegal acquisition and use of information; unauthorized access to information resources; manipulating with information; illegal copying of data in the information systems, etc.);
- "Trolls." (In the communities of social networks in the Internet so-called "trolls" who are the users distributing distorted, incorrect but profitable for one or the other lobbyists information started to work for hire);
- Visualization. (Even more information is presented in the form of visual images in the modern media (traditional and new ones));
- Psychological addiction. (Even more people feel psychologically addicted to processes taken place in the media environment);
- Deprivatization. (Intrusion upon one's private life);
- Governance of media. (People get even more inlined with comprehensive and quick-operating communication network having even fewer possibilities to influence the volume of information circulating inside it, quick-operation tempo or control them);
- Institutional dependence. (Dependence of social institutes on mass media increases);
- Immorality. (Modern Internet supports the users' wish to obtain through its services information, distribution of which is limited by the rules of morality and laws in the traditional mass media).

The high level of solidarity of all the groups of respondents should be noted. The points of view of men and women, representatives of different age groups and different cities not quite differ.

There are obviously some differences. The respondents of the elder age group less than the other are inclined to think that the media addiction has become a real threat of integrity, social adequacy of a person in the modern world; that even more people are felt psychologically addicted to processes happening in the media environment; that the uncontrolled access to information is dangerous; that mass media can be accused of breaking moral principles. At the same time the representatives of the youngest age group have doubts concerning the statement that the life success of a modern person is to a large extent defined by the number and quality of his/her presence/representation in the Internet. There are as well some other insignificant differences in the points of view.

The level of education also influences attitude to media threats to some extent. Thus, for example, the respondents with the higher technical education are less than the participants of the polling survey with the other education inclined to accuse mass media in blocking and poisoning the children's and teenagers' minds. The respondents with the higher journalism education are to a greater extent than the other participants of the polling survey inclined to agree with that the life success of a modern person is to a large extent defined by the number and quality of his/her presence/representation in the Internet as well as with the fact that the uncontrolled access to information is dangerous.

Employment of the participants of this polling survey in different sphere of social life not significantly but also influences the evaluation of significance of different media threats. It should be noted that from the perspective of the representatives of government authorities (in comparison with the other respondents) the fact that the modern Internet supports the users' wish to obtain through its services information, distribution of which is limited by the rules of morality and laws in the traditional mass media, is

not quite a problem. The participants of polling survey employed in the government authorities also do not consider the fact that execution of modern common performance project often creates just illusion of that the participation in the communities of social networks in the Internet promotes forming and development of civil society is quite a significant threat. The respondents employed in the sphere of material production share this point of view.

The representatives of the service industry taken part in this polling survey to a lesser extent than the other respondents think that the activity in the cyber world does not promote civil activity in the real world; that virtualization of political activity of the citizens rather hinders civil activity and conscious participation of the Russian citizens in the political process as well as that the modern media damage psychic of the people, form feeling of fear and despair.

The representatives of social organizations agree to a greater extent with the statements that the web-sites with such deviant information prevail in the Internet. But they are those who are lesser concerned with the fact that information and communication inequality among the regions increases in Russia. The significance of this media threat is the most realized by the respondents employed in the sphere of material production.

Job title of the participants of this polling survey does not virtually influence the evaluation of significance of different media threats. Except for the fact that the representatives of Senior Management are to a lesser extent than the participants of the polling survey with the other job title inclined to emphasize such threats as: "Uncontrolled access to information is dangerous"; "Mass media is guilty in blocking and poisoning of the children's and teenager's minds"; "Mass media can be accused of breaking moral principles"; "Modern media environment promotes breaking of traditional culture and systematic social and cultural crisis in Russia."

There is also no evidence of significant difference concerning significance of the presented media threats by the respondents from different cities of Russia where the study was conducted.

3.2. All the ways to Minimize Damage are Good. But some are the Best

The respondents were offered to evaluate a potential efficiency of different ways to minimize the media threats, the list of which was also formed based on the results of analysis of the expert survey.

1. Activation of possibilities of civil society in promotion of ideas concerning media environment protection (organization of social movements, etc.)
2. Ensuring compliance with the high ethical standards in the field of media activity
3. Provision of efficient access of the citizens to necessary information and resources of communication
4. Development of strict standards for provision of information security of a person and society
5. Development and realization of the methods of efficient protection of digital information
6. Development and realization of the state information policy based on the idea of environmental protection approach to the sphere of information
7. Development and realization of the national media education program (training the citizens on technologies of individual protection from media impact)
8. Execution of large-scale studies with the purpose of development recommendations on environmentally adequate interaction of people with the media environment
9. Forming of consciousness of the protected information environment by the citizens.

It should be noted that almost all the offered ways to minimize the media threats were widely supported by the participants of this polling survey. But from the perspective of the majority of respondents the following are the most efficient ways:

- Provision of efficient access of the citizens to necessary information and resources of communication;
- Development and realization of the methods of efficient protection of digital information;
- Ensuring compliance with the high ethical standards in the field of media activity;
- Development and realization of the national media education program (training the citizens on technologies of individual protection from media impact).

And in this case the respondents' solidarity is rather high. There are no significant differences among the men and women. The points of view of the respondents belonging to different age groups are close. A little prevalence among the respondents of the elder age group of such ways to minimize the media threats as "provision of efficient access of the citizens to necessary information and resources of communication"; "development of strict standards for provision of information security of a person and society"; "development and realization of the methods of efficient protection of digital information" can be noted. They also consider activation of possibilities of civil society in promotion of ideas concerning media environment protection and development and realization of the national media education program less significant that the participants of this polling survey of the other age.

The level of education has no significant impact on attitudes of the participants concerning ways to minimize the media threats, as well. Although the respondents with the secondary education think that the least efficient will be such ways as: "Ensuring compliance with the high ethical standards in the field of media activity" and "development of strict standards for provision of information security of a person and society."

The field of the respondents' work does not influence the points of view concerning purposefulness to use one or the other ways to minimize the media threats, as well. Job title of the respondents does not also influence their attitude to different ways to minimize the media threats.

There is the same situation concerning frequency of the Internet use. The only that is worth regarding is that development and realization of the state information policy based on the idea of environmental protection approach to the sphere of information as

the way aimed at minimizing the impact of media threat is accepted to a large extent by the respondents who use the Internet every day.

Neither duration of time spent in the Internet, or the purpose for the Internet use influence attitudes to potential ways to minimize the media threats.

As to the attitude of possible efficiency of the offered ways to minimize the media threats of the participants of polling survey resided in different cities it can be concluded that similar to the situation with evaluation of different media threat significance the respondents from different cities show high level of solidarity concerning the ways to their minimizing.

Curiously that (Table 6) the respondents accept reasonable to use almost all the specified ways to minimize the damage caused by them on some media threats approximately in equal quantities (for example, threats 7 and 10); and in relation to the other (for example, threats 1, 12, 30) the ways obtained over 30% of scores came through; the ways that were accepted by the respondents as absolutely inefficient were defined concerning the range of threats (for example, for threats 12, 17, 25, 30).

Table 6: Matrix of the most efficient ways to minimize definite threats from perspective of the participants of the polling survey

Threats	Ways to minimize media threats								
	1	2	3	4	5	6	7	8	9
1	X				0				
2		x					X		
3		X						x	
4			X	x				x	
5		x	X		0	0			
6		x					x		X
7	X				0	0	X	0	X
8							x	X	X
9		x		X					
10	X								x
11		X	x				x		
12	0					0	0	0	X
13		x	0	X					
14			X					X	
15				X	x				
16		x		X					
17		0	X	0	0	x			
18		X		0					
19									X
20		X						X	
21		X				x			
22		X	x						
23		X							x
24								X	
25	0	X	0		0	x			
26		X						x	
27				X					
28		x					x		X
29				X					
30	x	0	X	0	0	0	0	0	0
31							X		
32								X	
33	0		X			0		0	X

X: Main ways; x: Additional ways; 0: Inefficient ways

4. DISCUSSION OF THE RESULTS

Thus, it can be concluded that the number of peculiarities of the modern media perceived by different groups of audience as the threats is significantly less that the list offered by the experts. As to the ways to minimize the media threats the ones the most intensively supported by the citizens are provision of efficient access of the citizens to necessary information and resources of communication; development and realization of the methods of efficient protection of digital information; ensuring compliance with the high ethical standards in the field of media activity; development and realization of the national media education program (training the citizens on technologies of individual protection from the impact of media).

Both the list of media threats and the specification of the ways to minimize them sharply differ with the content of the above mentioned Information Security Doctrine that was approved by the Order of the President of Russia in September, 2000. Based on this Doctrine the Federal Service for Supervision of Communications, Information Technology, and Mass Media or Roskomnadzor was founded. This administration has obtained the right to caution the information resources for placement of the materials forbidden in the territory of Russia. By the end of 2013 the common list of illegal information with definitions and criteria concerning forbidden materials was created through joint efforts of Roskomnadzor, the Federal Drug Control Service and Rospotrebnadzor (the Federal Service for Surveillance on Consumer Rights Protection and Human Wellbeing). According to the Head of Roskomnadzor Alexander Zharov in the year 2014 the total number of web-sites added to the Common Register of Forbidden Information exceeded 45 thousands. 64% resources of them were caught in advocacy and distribution of drugs, 15% of them - in child pornography, 12% of them - in suicide (Smolyan et al. 1996).

Then the attention of the officials was drawn to piracy content in the networks. In August, 2013 the anti-piracy law came into force and it binds the Internet-resources to delete unlicensed music, films, books and other intellectual property after an appeal of the rights holders.

In the year 2014 popular figures in the Internet were subjects of attention of the government authorities. The Law on Bloggers came into force in August of that year prescribing all the figures concerning blogs and social networks with daily audience of over 3 thousand visitors to register as mass media. Thus, the owner of such a page or web-site is obliged to comply with the same laws and restrictions applied to mass media.

One of the latest headline steps in the field of information control in the Runet was an approval of the Law on personal data that came into effect on the 1st of September, 2015 and now all the foreign companies are obliged to store data concerning Russian users in the territory of Russia.

As the analytics note all the steps on control over the Russian segment of the Internet quite comply with the tasks set in the

information security doctrine. The authorities protect the Russian citizens from the hazardous information, protect the rights for intellectual property as well as control the activity of the foreign companies in relation to the citizens of Russia (Smolyan et al., 1996).

But there is the other point of view. The Chief Analytic if the Russian Association of Electronic Communications Karen Kazaryan supposes that the understanding of notion "information security" in Russia differs from its understanding accepted in the whole world. "If we judge in accordance with the globally accepted criteria then the situation is not quite optimistic. Russia is still the one of the leaders concerning the number outgoing hacker attacks, financial fraud, distribution of malware and tools for cracking. And the authorities do not take almost any measures to solve this problem and establish international cooperation in this field," the expert notes (Smolyan et al., 1996).

If we will talk about control over the cyber environment on part of the state, then according to Kazaryan the range of laws cleaning the Runet from troublesome information was passed in this field. "But the majority of them either becomes the tool in the hands of the local officials willing to advance or become highly-publicized in mass media that creates illusion of efficient work of the surveillance agencies," the expert thinks.

This gives ground to suppose that the paradigm of media security provided in the Information Security Doctrine is close to exhaust its heuristic potential. The deep problem of an approach from the point of view of security is in the fact that sooner or later this approach will lead to deadlock as to provide complete security under conditions of the society of risk is essentially impossible. The main drawbacks of this approach can be formulated in the following way.

It is supposed that the hazard of threats and, as a consequence, the threats, from which the protection is needed, are defined by means of risk analysis that is essentially correct. The problem is that no matter how experienced and educated the experts making decisions on the importance of one or the other media threats are, they will pay attention to some limited number of threats and significantly greater number of really existing media threats will be neglected due to the following reasons: (1) Low evaluation of the real nature of threat at the moment of analysis; (2) restricted abilities of people in perception of complicated systems, the modern media environment is belonged to; (3) complications in creation of quite adequate forecast models; (4) impossibility to forecast emersion of new threats and the consequences of their impact on society and a person.

But the main hazard of such approach is that the importance of the media threats, for achievement of protected state of which an unreasonable part of the resources available (potential) in the system can be used, is overestimated. As a consequence, the potential can be so undermined that the system will be vulnerable to emerging or previously neglected threats (Kurilo and Streltsov, 1995).

Thus, it is obvious that the other paradigms should replace the paradigm of media security. For example, in the international documents it is even oftener referred to forming competence (knowledge, abilities, skills) summarized in the term "media and information literacy" and providing for safe and responsible, based on critical thinking, use of the networks for free access, creation and exchange of information and knowledge within all language, culture and social groups. Necessity of such kind of competence becomes even more vital under conditions of the modern information environment contaminated with unreliable, unsafe and often malicious content (Skvortsov, 1995).

So, recognizing potential harmfulness of the media content the supporters of this paradigm consider possible to talk not about provision of security of different subjects from such content but about an increase of media and information literacy of the population that will allow people to protect themselves.

At present, apart from the paradigm of security and the paradigm of media and information literacy, an approach, the supporters of which make the principle of efficient development of information and communication environment a cornerstone, is formed. Thus, for example, in the Sakhalin Declaration "The Internet and Social and Cultural Transformations" it is noted that the concept of traditional institutes and existing legislation in the field of copyright protection guaranteed by the Universal Declaration of Human Rights need significant review with due regard to peculiarities of use, consumption, creation and distribution of works and services in the digital environment for the purposes of provision free access to information necessary for life, obtaining quality education, social and scientific development (Skvortsov, 1995).

Methodological basis of this approach can be the theory of stable development that has perhaps become not only the most studied, quickly developing and popular new theory of the last decade (hundreds of conferences, thousands of monographs, textbooks, etc.) but quite a "practical" one - all the developed countries of the world express their striving to follow direction to stable development and essentially all to some extent conceptual and "respecting themselves" official state and international documents use the notion of stable development as the base ideology for the last years (Veprintsev et al. 2003; Kononov, 2015).

5. CONCLUSION

The weight of evidence suggests that after 15 years of realization of the Information Security Doctrine in a particular country, Russia will again have to return to understanding of the media threats as a global phenomenon requiring the same number of global solutions. And these solutions should be based on not only and rather than prohibitions and punishments but on development of the society of knowledge founded on the humanistic values and four fundamental principles reflected in the UNESCO Constitution: Promotion of freedom of expression in traditional and new media including the Internet; availability of quality education for everyone; respect to cultural and language diversity; universal access to information and knowledge, in particular, to the information being a public domain.

The special attention should be drawn to development and promotion of ethical and legal principles and norms of behavior aimed at provision of not only state but the public interests in the sphere of information. And the state policy in the field of information should aim at support of inclusive social development and promotion of intercultural dialogue. This activity should be carried out by means of strengthening the right for use of information and new communication means (including hardware and software) and widening the possibilities of the citizens through development of knowledge, skills and attitudes that will allow them to execute these rights to full extent.

And, surely, all the parties concerned should in every way promote formation of the training and educational programs, especially for the youth concerning social and cultural transformations (ethical, legal, cultural and social aspects of digital communication and media) caused by the use of modern information and communication technologies and the Internet. Such programs should also aim at an increase of awareness concerning meaning of new terms connected with the emersion of the information society and the society of knowledge. This will promote expending of possibilities and an increase of the citizens' competence in media and information sphere that will allow efficient, safe and responsible use of information and communication technologies and the Internet (Skvortsov, 1995).

Realization of these and other ideas stated in the international documents will allow bringing together the statist understanding of information and media security of the essence put in these notions by the citizens of Russia.

6. ACKNOWLEDGMENTS

This publication was prepared within the frameworks of scientific project No. 15-03-00514 powered by the Russian Foundation for Humanities. The Program of joint financing of grants of the Russian Foundation for Humanities of the Scientific Foundation of National Research University Higher School of Economics.

REFERENCES

Declaration on the Environment and Development. (1992), Approved by the UN Conference on Environment and Development. Rio de Janeiro. Available from: http://www.un.org/ru/documents/decl_conv/declarations/riodecl.shtml. [Last retrieved 2015 Oct].

Doctrine of Information Security. Available from: http://www.fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/111-tekhnicheskaya-zashchita-informatsii/dokumenty/kontseptsii/374-doktrina-ot-9-sentyabrya-2000-g-n-pr-1895.

Federal Law of the Russian Federation dated December 29, 2010 No. 436-ФЗ "On Protection of Children against Information Harmful to Their Health and Development." (2010). Available from: http://www.rg.ru/2010/12/31/deti-inform-dok.html.

Grachev, G.V. (1998), Information and psychological security of person: Condition and possibilities of psychological protection. Moscow: Publishing House of Moscow University.

Grachev, G.V., Melnik, I.K. (1996), Methods and techniques of the manipulative influence in mass information processes. Problems of Information and Psychological Security (Collection of Articles and Materials of Conferences). Moscow: Institute of Psychology of the Russian Academy of Sciences.

Polyaeva, N.K, Sokolova, E.P., Minbaleev, A.V. (eds.) (2005). Human in the Media World. Security in the Mass Communication. Chelyabinsk: Tsitsero.

Information and Psychological Security in the Mass Media. (2002). Moscow: Aspekt-Press.

Johannesburg Declaration on Sustainable Development. (2002), Adopted at the 17th Plenary Meeting of the First World Summit on Sustainable Development, Johannesburg. Available from: http://www.un.org/ru/documents/decl_conv/declarations/decl_wssd.shtml. [Last retrieved on 2015 Oct].

Kononov, A.A. (2015), To the new paradigm of security: Security as competitiveness. Available from: http://www.mirozdanie.narod.ru/Authors/SecComp.html. [Last retrieved on 2015 Oct].

Kurilo, A.P., Streltsov, A.A. (1995), Information Security and Regional Policy of the Russian Federation. Problems of the Global Security: Materials of Seminars within the Framework of the Research and Information Program, November, 1994-February 1995. Moscow.

Pilgun, M. (2015), Basic communication pattern in Russian network environment. Journal of Psycholinguistics, 2(24), 176.

Pilgun M., Gradoselskaya G. (2015) Political Communication on Facebook: Russian Case. Revista Latina de Comunicación Social, 70, 726-749.

Pozdnyakov, A.I. (1994), Information security of person, society and state. Bezopasnost, 5, 29-39.

Problems of Information and Psychological Security (Collection of Articles and Materials of Conferences). (1996), Moscow: Institute of Psychology of the Russian Academy of Sciences.

Roshchin, S.K., Sosnin, V.A. (1995), Psychological security: New approach to the security of person, society and state. Rossiyskiy Monitor, 6, 133-146.

Sakhalin Declaration "Internet and Socio-Cultural Transformations". Available from: http://www.mcbs.ru/documents/1/308/. [Last retrieved on 2015 Oct].

Shestoperov, D., Todorov, V. 15 Years of the Information Security. Available from: http://www.gazeta.ru/tech/2015/09/09/7747157/information_security_turns_15.shtml. [Last retrieved on 2015 Oct].

Skvortsov, P.V. (1995), Information Culture as a Condition of the Mankind Survival. Problems of Global Security: Materials of Seminars within the Framework of the Research and Information Program, November, 1994-February, 1995, Moscow.

Smolyan, G.L., Zarakovskiy, G.M., Rozin, V.M. (1996), Information and Psychological Security (Determination and Analysis of the Subject Domain). Moscow: Institute for System Analysis of the Russian Academy of Sciences.

UNECE Strategy for Education for Sustainable Development. (2005), Adopted in Vilnius. Available from: http://www.ecoculture.ru/ecoeducation/development/docs.php. [Last retrieved on 2015 Oct].

Veprintsev, V.B., Manoylo, A.V., Petrenko, A.I., Frolov, D.B. (2003), Operations of the information and psychological war: Methods, aids and technologies. Concise Encyclopedic Dictionary. Moscow: Goryachaya Liniya – Telekom.