Information and security components of the Russian foreign policy

Mariia Zaitseva

Post-Graduate Student
Institute of International Relations
Taras Shevchenko National University of Kyiv
36/1 Melnikova Str., Kyiv, Ukraine, 04119
E-mail: mariya.zaitseva@gmail.com

The aim of the paper is to examine the Russian Federation's doctrines in the sphere of information security. Such analysis allowed to lay down the information and security strategy of the state in the international arena and to study the specifics of the Russian model of information security. It was also determined that in order to counteract information threats, the Russian political administration continues an active development of cooperation with such actors as SCO and BRICS which de jure keep the neutral position concerning the Russian–Ukrainian relations, but de facto continue to expand economic cooperation with the RF. In the article, reviewed are the instruments of Russia's modern information and propaganda operations, which were used in Chechnya and Georgia, and the specifics of propaganda operations against Ukraine are analysed.

Keywords: *information security, foreign policy interests, Russia, Chechnya, Georgia, Ukraine, CIS, SCO, BRICS.*

Introduction

In the beginning of the 21st century, the structural crisis of the system of international security appeared especially noticeable in the context of inadequate reaction to new challenges and threats which emerged with the formation of the global information society. It resulted in the necessity to reconsider the conceptual and methodological principles of international cooperation in the field of information security, determination of the interference of global development and information security, a clear differentiation of the priorities of global, regional, and national policy as to modern information threats. The efficiency of methods and instruments of information conflict is confirmed in practice as modern methods of information confrontation are able to result in a loss of national idea, spiritual and material values, change of the social structure and political system, disintegration of a state and army, the economic crisis or the intensification of ethnical and confessional contradictions. Combination of traditional forms of information confrontation with the latest achievements in the sphere of information technologies began considerably influence the course and result of the conflict resolution (Chernyk, Shumka, 2008).

The analysis of foreign and Ukrainian researches confirms the transformation of approaches to understanding the place and role of information security in international cooperation. A special contribution to the comprehension of information security as a political category belongs to such foreign and Ukrainian scientists as I. Wallerstein, J. Arquilla, M. Castells, M. Libicki, R. Keohane, H. M. McLuhan, J. Nye, A. Krutskih, O. Leonov, I. Panarin, A. Hutsal, M. Ozhevan, V. Lipkan, O. Lytvynenko, Eu. Makarenko, Hr. Perepelytsya, G. Pocheptsov, M. Ryzhkov, D. Dubov. The further analysis of the security component in foreign policy interests of the Russian Federation will allow to reveal the strategy of using information and propagandist operations to support one's own influence on the international stage.

The Russian model of information security

The current geopolitical situation, according to Russian experts, requires a fundamentally different approach to the issue of national security protection in Russia and to the analysis of the content and evolution of the whole range of geopolitical factors, the most important of them being information. Currently, it is arguable that the country's achievement of strategic benefits depends on its existing information resources. The objects of information and psychological protection of national security, as emphasized in the research projects, are the information-psychological sphere of society, which is part of the global information environment and is related to the use of information, information resources, and information infrastructure to influence the mind and behavior; information resources, especially spiritual, cultural, historical, national values, traditions, etc.; the system of social consciousness formation; the system of public opinion formation; the system of political decision-making; the human mentality (Grachev, 1998; Grinyaev, 2004; Panarin, 2006).

Researchers believe that the concepts of "information confrontation" and "information warfare" are not identical. They define information confrontation as a complex joint use of forces and means of information confrontation and armed struggle. Information warfare, as opposed to the armed struggle, is conducted both in peace- and wartime. The Russian researcher I. Panarin identifies two types of information confrontation in the military sphere: information-technological and information-psychological. The main objects of influence and protection during the information-technological confrontation are information technology communication systems, telecommunication systems, radio-electronic devices, etc. The main objects of the influence and protection in the information-psychological confrontation are the psyche of the armed forces, intelligence services and people of opposing sides; systems of decision-making and public opinion formation (Panarin, 2006).

The Russian model of information security is to create the favorable domestic information environment through the use of media holdings to manipulate public opinion. This model is aimed against potential and genuine internal and external information-psychological threats, but is less effective against cyber attacks. The main characteristics of the model, according to researchers, are heavy censorship, crudity and vagueness of the relevant legislation, the lack of transparency of relations between the government and the media, the lack of balance between the ruling and the opposition media, the politicization of mass media (Zasurskij, 2001).

The Representative of the Conflict Studies Research Centre Oxford K. Giles has observed that the Russian views on the nature, potential and use of cyberspace differ significantly from the Western consensus. In particular, Russia has deep concerns as to the principle of uncontrolled exchange of information in the cyberspace and the presumption that national borders are of limited relevance there. The circulation of information which poses a perceived threat to society or the state, and the sovereignty of the "national internet", are the key security concerns in Russia. Russia will continue to push international agreements regulating the cyberspace, along the lines of the consensus already achieved with like-minded states in the CSTO, SCO, and BRICS (Giles, 2012).

Formation of national information field of Russian Federation: doctrines

At the beginning of the 21st century, the government of the Russian Federation began consecutive politics in the restoration of the state's unity through the formation of the national information space. The problems of the information security of the state are outlined in the *Information Security Doctrine* of the *Russian Federation*, which was approved on the 9th of September, 2000, and which became the first state program of Russia to regulate the sphere of information security (Security Council of the of Russian Federation, 2000). A new push for the development of Russia's national strategy of information security was the document "The Basis of the Russian Federation State Policy in the Sphere of International Information Security to 2020", which was signed by the RF President in 2013 as an answer to the U.S. *International Strategy for Cyberspace,* released by the White House in 2011. The document was worked out by the Russian Federation Security Council in cooperation with the profile ministries, including the Ministry of Foreign Affairs, Ministry of Defense, Ministry of Communications and Mass Media, and Ministry of Justice (Security Council of the of Russian Federation, 2013). It should be stressed that it is the first official document which legally establishes Russia's information security policy.

In particular, the doctrine includes four basic information security threats for the Russian Federation: 1) the use of ICT as an information weapon for the military and political purposes; 2) the use of ICT in terroristic actions; 3) realization of cyber crimes; 4) the use of Internet technologies with the aim to intervene in the internal state affairs, to provoke public order disturbances, to propagandize violence and stir up hostility. The active cooperation between Russia and international partners within SCO, BRICS and the initiation of the process of adoption of international norms of behavior in the Internet, which would function on the basis of a single network control system, are provided for in the document in order to counteract information threats. The Ministry of Defense of the Russian Federation, Federal Agency of Government Communications and Information under President of the Russian Federation, Federal Security Service, Joint Committee on Information Security under the Security Council of the Russian Federation and the Administration "K" of the MIA of the Russian Federation are actually involved into studying the problems of the information war (Security Council of the Russian Federation, 2013).

On the 5th of February, 2010, the Military Doctrine of the Russian Federation was adopted, which Russia prepares to update in order to comply with such international and political challenges as the NATO expansion, renewal of the ABM system, negotiation of the Ukrainian crisis and fight against its consequences for the Russian Federation (Dede, 2014). "Russia's National Security Strategy to 2020" was ratified for the achievement of foreign policy interests and the strengthening of positions. It is stated that threats in the field of information security can be overcome through improvement of security of information and communication systems' functioning of critically important objects of infrastructure and high-risk facilities in the Russian Federation, enhancement of the security level of the corporate and individual information systems, establishing a single system of information and communication support for the system of national security protection (National Security, 2009).

It is underlined in the Strategy that in the medium-term the Russian Federation needs to overcome the lag in technology in the important spheres of informatization and telecommunications, which determine the state of national security, to work out and implement technologies of information security in the systems of state and military administration, systems of control over ecologically hazardous production facility and critically important objects, and also to provide terms for the harmonization of the national information infrastructure with the global information networks and systems (National Security, 2009).

Modern information and propagandist operations of the Russian Federation

Chechen, Georgian, and Ukrainian information and propagandist operations are the displays of ensuring foreign-policy interests by the Russian Federation. In particular, the Chechen campaign in the informational aspect had an absolutely new quality format both in the part regarding work with the own troops and population and the influence on the opponent (Zyrfa, 2009). The Chechen conflict was called the "first Russian television war". However, experts underline that Russia lost this campaign, first of all in the information field, because the military forces didn't accomplish their task adequately, what allowed journalists infiltrate into the lines of the terrorists who posed for the cameras and gave interviews. Besides, there was no special staff representative for contacts with public and mass media (Strizhenko, 2003).

During the second military campaign in Chechnya, the government held a tight hold on the internal exchange of information about the conflict. The Russian Security Council Secretary invoked the mass media to conduct the infowar against Chechen terrorists stepwise and not produce interviews with mercenaries. The specialists also outlined such forms of control over the information space during the Chechen campaign as control over verbal messages, control over visual pictures, according to which TV shouldn't show the pictures of the wounded, loss of military hardware by federal troops, and control over the unity of interpretation; in this case, it was forbidden to demonstrate on TV any interviews with mercenaries (Strizhenko, 2003).

Thus, for the western audience ideology of anti-terrorist operation which successfully fits the western world model was actively generated. Russia tried to achieve the permanent leading in information confrontation, simultaneously using the experience of western countries in resolving the Kurdish, Basque, Corsican, Iraqi conflicts. The information and propagandist measures regarding the defence of troops and population secured all stages of the operation and were conducted for the support of the authority of the Russian Federation military forces, forming the public opinion, for the support of consolidated actions by troops, informing about the absolute consent and mutual understanding of local authorities, population and force structures which participate in the operation, demonstration of readiness to keep Chechnya within the confines of Russia, informing the Daghestan and Chechnya population about the events of social, humanitarian, civil defence, which were accepted by the Russian government military operations (Chernyk, Shumka, 2008).

According to Western researchers, the Chechnya war has influenced the Russian mindset and brought practical knowledge and insights to the Russian approach to information warfare. Both wars in Chechnya showed that in some areas even a small and relatively impoverished adversary could achieve information dominance over a stronger opponent by using the mass media component efficiently. One of the greatest successes of the Second Chechen War was Russia's ability to manipulate the media. Western scientists believe that the Russian media will be a powerful asset in the future Russian information operations (Thomas, 2003; Renaud, 2010).

The open support of the puppet separatist groups in Abhazia and South Ossetia became the new element of the Russian foreign policy. In particular, Russia used the Kosovan precedent for the identical solution of frozen conflicts in the CIS. Providing connection of the population of Abhazia and South Ossetia with their "historical homeland" Russia actually exercised the right of defence of citizens, having started military operations against Georgia. Manipulating the fact that about 90% of Russian citizens live on the territory of South Ossetia, the speaker of the State Duma of the Russian Federation at the beginning of the military campaign noted that "Russia would not give up full-scale actions in this region, if they were necessary to protect Russian citizens and maintain safety on the south borders" (Zyrfa, 2009).

With the aim to show Georgia as an aggressor state, in the information field there appeared messages about bringing the military technique of the armed forces of Georgia into South Ossetia. For this purpose, news anchors emphasized the "atrocities" of Georgian soldiers who killed injured Ossetians and Russian peacemakers, without any corresponding photo- or video proof materials. In addition to that, there was made an attempt to form a positive image of the Russian Federation authorities; in particular, the mass media covered such events as an urgent arrival of the Russian Prime Minister to the North Caucasus from Beijing where he attended the Olympics Opening Ceremony, and bringing troops of the 58th army of the Russian Federation Armed Forces on the territory of Georgia. Up to that, there appears the term "peace enforcement of Georgia", which is motivated by the unwillingness of the Georgian authority to sit down at the negotiating table. During the military operation, considerable part of telecasts was produced exactly for an external audience. The Russian federal TV channels transmitted similar stories through the satellite television, trying to create favourable conditions to justify bringing troops into Georgia, presenting Georgia as an aggressor, creating a positive for the Russian Federation picture of actions in Tskhinvali and in the separatist region. There were also conducted few cyberattacks in the Internet network; in particular, with the beginning of military activities the official website of the Georgian MFA to Georgia stopped its functionig; instead, on the main page of the website the visitors could see a set of the photos of Georgian President M. Saakashvili compared with A. Hitler; some governmental websites were blocked or access to them was limited. The actions of intimidation were widely practiced; especially, on the basic Russian websites were placed videos on which the Georgian army took losses, a lot of photos with dead Georgian soldiers, and on the completion of military actions – the captured military technique and prisoners (Leczkalyuk, 2012).

Exploring the war in Georgia and the reaction of the West, the Western scholar M. Bowker wrote that Washington's alliance with Georgia was sufficiently close to make President Saakashvili believe he would receive American support in the event of war with Russia. The war, however, was not in America's interest since it threatened its position in the South Caucasus and provided Russia an opportunity to re-emphasize its growing power in the world (Bowker, 2011).

The information and propagandist operation of the Russian Federation against Ukraine began in spring 2008 after V. Putin had made a statement at the NATO summit in Bucharest: "Ukraine, as it exists today, was formed in the Soviet time. Ukraine received the Crimea by the decision of the Political Bureau of the CPSU. 90% of its population are Russians. Who can tell us that we have no interests there?.." (Zyrfa, 2009). The extensive infowar of the Russian Federation against Ukraine, which started in November–December 2013, was aimed to discredit the Maidan among the Western society and citizens of the Eastern regions of Ukraine. Thus, the Russian TV channels presented the situation in Simferopol by the videos from the EuroMaidan, published the untruthful information that Ukrainian soldiery came over Russia and reported about large queues of Ukrainian refugees who were standing near the Russian border. A special attention was given to the image of Maidan activists as extremists. Another element of the campaign is aggressive manipulations by Russia at the issues of language and rights for national minorities, in particular Russians in the Crimea and on the East of Ukraine. Thus, the Russian Federation gave out the idea that the Maidan became the revolution of Ukrainian nationalists, stacked against the rights of national minorities. The coverage of events in the Crimea looked like the demonstration of force rather than a military operation, because information messages in the Russian media about the invasion and seizure of military objectives by Russian soldiers or the panic of the Russian-speaking population in Eastern Ukraine contradicted the reality (Philipchuk, Zaharova, Prytula, Kovalchuk, Pol, 2014).

After annexation of the Crimea, the next stage of information operation, the final task of which is the achievement of its own foreign-policy aims in Ukraine, is control over the territory of Ukraine or its parts for the sake of maintenance of a buffer zone that would separate Russia from the direct contact with the NATO. The beginning of this stage was the armed seizure on the 6th of April, 2014 of the regional state administrations in Donetsk and Kharkiv and the building of the State Security Service of Ukraine in Luhansk. At the same time, in the Russian-language information space there was started the introduction of messages about an inevitable intensification of the wide-range "civil war" in Ukraine. Such rhetoric became even more aggressive after Ukraine had announced an anti-terror operation on the Eastern territories of the country. Consequently, special attention to the realization of its own foreign-policy aims Russia pays to the information content. The aim of such information operation is to weaken the moral and material forces of the Ukrainian side and to strengthen its own ones, and to impose on Ukrainian citizens the idea of the illegitimacy of Ukrainian government of, the necessity of the country's federalization, the balefulness of the European vector of development, disorientation and disinformation of the population in the Eastern and Southern regions, the weakening of belief in the necessity of maintaining the Ukrainian unity, influence on the decision-making process, intimidation of Russians by the enemy image as "Banderites" from Ukraine (Ryabyh, 2014).

It should be emphasized that in the realization of information operation in Ukraine, Russia paid attention to mass media as to the basic instrument in achieving its foreign-policy aims, which is able to complement the political, economic, diplomatic instruments of its influence. At the same time, the Russian secret-service and diversionary-intelligence groups that act on the Ukrainian territory are considered as an important military component and the instrument of influence on the local community by producing news with their further use to enhance the "information battlefield". The subjects of information influence are both the population of Ukraine and the population of the Russian Federation, the loyalty of which guarantees the maintenance of the existing Russian political regime for some time. For strengthening the information influence on both the population of the Russian Federation and on the citizens of the Eastern regions of Ukraine openly untruthful or considerably corrupted information is used. Through the implementation of such stamps, conditions are created for rousing separatism in Ukraine and support by the Russian population defense of the Russian-language minority in Ukraine by Russian authorities (Ryabyh, 2014).

The Polish researcher J. Darczewska expresses the opinion that using the methods inherited from the Soviet times, Russia has managed to transform the real Ukrainian–Russian conflict and military intervention into a virtual conflict between Russia and the West. In her work, J. Darczewska soundly argues that Russia has now revealed its geopolitical ambitions and has set out to impose its way of thinking in terms of geopolitical blocs while forcefully delineating the border between the "Russian world" civilisation and the West. The West's relations with Russia have entered a new, colder phase. Improving relations would require the Russian leadership to change its perception of the international reality and its thinking which is based on the politics of force and spheres of influence, and to abandon its ambition to delineate new civilizational divides (Darczewska, 2014).

International cooperation as the instrument of promoting the Russian foreign policy interests

After introduction of international sanctions by the EU countries and USA, and also the support of their actions by a number of other developed countries, Russia can gradually find itself in an economic and political vacuum which will result in a domestic crisis. To alleviate the consequences of sanctions, the Russian Federation launches a propagandistic campaign in the world media in order to discredit the Ukrainian political authority. Besides, it is important for the Russian Federation to find allies, in particular BRICS countries. Although *de jure* Brazil, India, China and the Republic of South Africa took up the neutral position in the question of flare-up between Russia and Ukraine, *de facto* these countries continued extension of their economic cooperation with the Russian Federation.

Thus, Russia, through the potential of BRICS, received an effective instrument of the realization of its own foreign-policy initiatives and national interests, one of which is the return of the former Soviet Union positions in the international arena. For this purpose, Russia formally advocates for coordination of efforts and unanimity of positions among BRICS countries regarding the questions of global stability, international and regional security, the strengthening of the coordinating role of the UN in the field of fight against international terrorism, fight against drug trafficking, cooperation for providing international information security and development of collaboration to control cyberterrorism and cybercrimes, and so forth (Sergeev, Alekseenkova, 2011).

Presently, the Russian initiatives regarding the international information security are promoted not only at the level of the UN, SCO and BRICS, but also within the framework of the CIS where the Russian Federation comes forward for the unification of the information space with the aim of a more effective realization of common interests, especially in the sphere of information security. The realization of the cooperation of CIS states was foreseen to be carried out in the form of mutual consultations, coordination and cooperation in the spheres of scientific researches, development and production of appropriate facilities for information security. In particular, it was planned to work out the international-legal mechanism of prohibition within the CIS of illegal information effects on personal and social consciousness; setting up of competent law-enforcement authorities on computer crime prevention; prevention and control of crimes in the information field. Such initiatives were not implemented within CIS, although the basic elements of the Russian conception of information security are put into effect through bilateral cooperation and on the level of national legislation (Makarenko, 2012).

Conclusion

The role and place of the information confrontation in the system of maintenance of national security gradually grows. The Russian Federation, in order to achieve its foreign policy aims, presently augments its information potential. Moreover, presently, international-legal norms under which information confrontation can be given the same status as crime are now absent. In connection with the accelerated development of electronic media, sharply increased the role of public opinion, which considerably influences social and political processes, specifics of the functioning of information and the psychological environment, the mental health of military men during armed conflicts. Therefore, the system of forming the public opinion is also one of the basic objects of information and psychological security of the Russian Federation.

Nowadays, Russia for the purpose of support and maintenance of its own foreign policy interests, has actively begun to use information instruments of the mass-media and social media. Understanding by the Russian authority the advantages of such instruments led the formation of laws in the field of information security, which regulate the control processes of the Russian-language information space. The Russian Federation Strategy in the use of modern information instruments for providing information influence on the opponent is not new but adopted from the USA and EU countries, complemented by the Soviet experience, hence the methods of counteraction to such information operations are also well-known. A barrier on the way of the effective counteraction to information and propagandist campaigns is the inconsistency of the positions of the political and military elite regarding the situation in the state, practical deficiency of information materials in the information field of the country which are designed to form a consolidated national idea, support of the artificial division of a country into “insiders and outsiders” by political elite, etc. Thus, each country can use, and does use, the information arsenal for the promotion of its own foreign-policy interests; however, the countries against which such “information aggression” is directed should be able not only to defend but also to conduct its own information operations.

REFERENCES

BOWKER, M. (2011). The war in Georgia and the Western response [interactive]. *Central Asian Survey*. vol. 30, no. 2, June 2011, p. 197–211 [accessed 15 January 2015]. Access through Internet: <http://www3.nccu.edu.tw/~lorenzo/Bowker.pdf.>

CHERNYK, P.; SHUMKA, A. (2008). Informacijno-psyhologichni operaciyi u vijnah ta zbrojnyh konfliktah drugoyi polovyny XX – pochatku XXI st. *Derzhava ta armiya*. L., № 634, p. 126–133.

DARCZEWSKA, J. (2014). The Information War on Ukraine New Challenges [interactive]. *Cicero Foundation Great Debate*. Paper No. 14/08, December 2014, 19 p. [accessed 15 January 2015]. Access through Internet: <http://www.cicerofoundation.org/lectures/Jolanta_Darczewska_Info_War_Ukraine.pdf>.

DEDE, O. (2014). Rusya'dan yeni askeri doktrin [interactive]. *Yeni Mesaj*. [accessed 10 November 2014]. Access through Internet: http://www.yenimesaj.com.tr/?artikel,12010894/rusya-dan-yeni-askeri-doktrin/orhan-dede.

GILES, K. (2012). Russia's Public Stance on Cyberspace Issues. [interactive]. *4th International Conference on Cyber Conflict,* NATO CCD COE Publications, Tallinn, p. 63–75 [accessed 15 January 2015]. Access through Internet: <https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf>.

GRACHEV, G. (1998). *Informacionno-psihologicheskaya bezopasnost' lichnosti: sostoyanie i vozmozhnosti psihologicheskoj zashhity*. M.: Izd-vo RAGS. 125 p.

GRINYAEV, S. (2004). *Pole bitvy – kiberprostranstvo: Teoriya, priemy, sredstva, metody i sistemy vedeniya informacionnoj vojny*. M. 426 p.

LECZKALYUK, M. (2012). Rosijs'ko-gruzyns'kyj konflikt: informazijne protystoyannya [interactive]. *Mors'ka derzhava*. № 31 [accessed 10 November 2014]. Access through Internet: <http://fleet.sebastopol.ua/morskaya_derjava/2008_31/rosijsko_gruzinskij_ konflikt_informatsijne_protistojannja/>.

MAKARENKO, Eu. (2012). Superechnosti spivrobitnycztva krayin BRICS u sferi informacijnoyi bezpeky: tendenciyi i perspektyvy. *Problemy mizhnarodnyh vidnosyn*, vol. 5, p. 356–371.

National Security: *Strategiya nacional'noj bezopasnosti Rossijskoj Federacii do 2020 goda.* Utverzhdena Ukazom Prezidenta Rossijskoj Federacii, 12 May 2009, № 537 [interactive], [accessed 10 November 2014]. Access through Internet: <http://www.scrf.gov.ru/documents/99.html>.

PANARIN, I. (2006). *Informacionnaya vojna i geopolitika*. M. 560 p. ISBN: 5-9763-0001-4.

PHILIPCHUK, V.; ZAHAROVA, O.; PRYTULA, V.; KOVALCHUK, Y. A.; POL, A. (2014). Zovnishn'opolitychni akcenty: rosijs'ka agresiya, mizhnarodna pidtrymka ta plan dij dlya Ukrayiny [interactive]. *Mizhnarodnyj centr perspektyvnyh doslidzhen'*. № 1 [accessed 10 November 2014]. Access through Internet: <http://icps.com.ua/pub/files/114/55/%D0%97%D0%BE%D0%B2%D0%BD%D1%96%D1%88%D0%BD%D1%8C%D0%BE%D0%BF%D0%BE%D0%BB%D1%96%D1%82%D0%B8%D1%87%D0%BD%D1%96%20%D0%B0%D0%BA%D1%86%D0-%B5%D0%BD%D1%82%D0%B8%20%20%E2%84%961.pdf>.

RENAUD, S. (2010) *A View from Chechnya: An Assessment of Russian Counterinsurgency During the two Chechen Wars and Future Implications*. [interactive]. New Zealand. 148 p. [accessed 15 January 2015]. Access through Internet: <http://muir.massey.ac.nz/bitstream/handle/10179/1804/02_whole.pdf>.

RYABYH, V. (2014). Podiyi na shodi Ukrayiny – drugyj etap polityko-vijs'kovoyi operaciyi shcho realizuyet'sya Rosijs'koyu Federaciyeyu [interactive]. *Defense Express* [accessed 10 November 2014]. Access through Internet: <http://www.defense-ua.com/rus/hotnews/?id=41611>.

Security Council of the Russian Federation: *Doktrina informacionnoi bezopasnosti Rossijskoj Federacii.* Utverzhdena Prezidentom Rossiiskoi Federacii 9 September 2000 [interactive], [accessed 10 November 2014]. Access through Internet: <http://www.scrf.gov.ru/documents/6/5.html>.

Security Council of the Russian Federation: *Osnovy gosudarstvennoi politiki Rossiiskoi Federacii v oblasti mezhdunarodnoi informacionnoi bezopasnosti na period do 2020 goda*. Utverzhdeny Prezidentom Rossiiskoi Federacii 24 July 2013, № Pr-1753 [interactive], [accessed 10 November 2014]. Access through Internet: <http://www.scrf.gov.ru/documents/6/114.html>.

SERGEEV, V.; ALEKSEENKOVA, E. (2011). *Perspektivy institucionalizacii BRIC (vklyuchaya rasshirenie povestki dnya)* [interactive], [accessed 10 November 2014]. Access through Internet: <http://www.brics.mid.ru/brics.nsf/WEBforumBric/C45997ED5B7E4CC4C3257859005A829B>.

STRIZHENKO, A. (2003). *Zarubezhnaya i rossiiskaya zhurnalistika: transformaciya kartiny mira i soderzhaniya*. Barnaul. 470 p.

THOMAS, T. (2003) *Manipulating the Mass Consciousness: Russian & Chechen information war. Tactics in the second Chechen–Russian conflict* [interactive], [accessed 15 January 2015]. Access through Internet: <http://call.army.mil/fmso/fmsopubs/issues/chechiw.htm>

ZASURSKIJ, Ya. (2001). Informatsionnaya bezopasnost' Rossii i sredstva massovoi informacii. *Informatsionnoe obshchestvo*. vol. 4, p. 19–23.

ZYRFA, Yu. (2009). Richnycya «novoyi zovnishn'oyi polityky» RF: chy vtilyuyut'sya v zhyttya zadumy Medvedyeva? [interactive]. Viche, №15 [accessed 10 November 2014]. Access through Internet: <http://www.viche.info/journal/1583/>.

RUSIJOS UŽSIENIO POLITIKOS INFORMACIJOS IR SAUGUMO KOMPONENTAI

Mariia Zaitseva

Santrauka

Darbo tikslas yra išnagrinėti Rusijos Federacijos doktrinas informacijos saugumo srityje. Tokia analizė leido padėti pagrindus informavimo ir saugumo strategijai valstybės tarptautinėje arenoje ir Rusijos informacijos saugumo modelio specifikai. Rusijos informacijos saugumo modelis yra skirtas palankiai vidaus informacinei aplinkai sudaryti, pasitelkiant žiniasklaidą, padėsiančią manipuliuoti visuomenės nuomone. Tačiau ekspertai teigia, kad toks modelis yra mažiau veiksmingas prieš kibernetines atakas. Taip pat buvo nustatyta, kad, siekdama užkirsti kelią informacijos grėsmei, Rusijos politinė administracija ir toliau aktyviai plėtoja bendradarbiavimą su tokiais veikėjais kaip ŠBO ir BRICS, kurie *de jure* išlaiko neutralią poziciją dėl Rusijos ir Ukrainos santykių, tačiau *de facto* toliau plėtoja ekonominį bendradarbiavimą su Rusijos Federacija. Straipsnyje peržiūrimos šiuolaikinės Rusijos informacinių ir propagandinių operacijų priemonės, kurios buvo naudojamos Čečėnijoje ir Gruzijoje, ir analizuojama propagandos operacijos prieš Ukrainą specifika. Siekdama realizuoti informacines operacijas Ukrainoje, Rusija atkreipė dėmesį į tai, kad žiniasklaida, kaip pagrindinė priemonė siekti savo užsienio politikos tikslų, gali papildyti politinius, ekonominius, diplomatinius įtakos instrumentus. Kad būtų sustiprinta informacijos įtaka Rusijos Federacijos gyventojams ir Rytų regionų Ukrainos piliečiams, naudojama akivaizdžiai neteisinga arba smarkiai iškreipta informacija. Taip sukuriamos prielaidos skatinti separatizmą ir kartu destabilizuoti politinę ir ekonominę padėtį Ukrainoje.