

**State Budgetary Educational Institution of Higher Education  
«RUSSIAN PRESIDENTIAL ACADEMY OF NATIONAL ECONOMY AND  
PUBLIC ADMINISTRATION»**

**CENTRAL RUSSIAN INSTITUTE OF MANAGEMENT - BRANCH**

*Manuscript copyright*

**TSARIK Vladimir Stanislavovich**

**CONSTRUCTION OF SYSTEM OF COUNTERING ‘RUSSIAN  
INFORMATION THREAT’ IN THE WEST (2014-2019):  
CONCEPTUAL AND INSTITUTIONAL ASPECTS**

5.5.4. International relations, global and regional studies

Abstract of thesis submitted for the degree of candidate in political science

**Supervisor:**

Candidate of Political Science,

Associate Professor

Malakhova Oksana Vladimirovna

Oryol, 2023

**The main results of the thesis of V. S. Tsarik**  
**«Construction of system of countering ‘Russian information threat’ in the**  
**West (2014-2019): conceptual and institutional aspects»**

The thesis presented by V. S. Tsarik for the academic degree of candidate of political science in specialty 5.5.4. “International relations, global and regional studies” contains self-sufficient complete research of conceptual grounds and institutional framework of the process of establishing system of countering ‘Russian information threat’ in the West in the period 2014-2019. The research work set forward a compact of findings that are imbued with scientific novelty, make an important contribution to Russian political science and possess practical value for elaborating state’s foreign and information policies.

**The relevance of the research topic.** In 2014-2021 Russia had been regularly accused in Western public rhetoric of using destructive means of information impact putatively constituting an extraordinary, almost existential threat to national security and social stability of the Western states. These accusations acquired not just a substantial media resonance but also an expert and academic justification and, subsequently, a political covering having turned into one of undisputable constants of the Western discourse and crucial component of an overall confrontation line towards our country that has been unfolded in the aftermath of 2014 crisis. Basing upon those accusations a whole system of countering ‘Russian information threat’ was erected consisting of formal and semi-formal state and inter-state arrangements and also of a huge network of non-state structures and instruments designed to detect and neutralize cases of dissemination by Russian government of disinformation, misinformation, propaganda and the so called ‘fake news’.

It was not a typical information war perceived as actions with a view to bring damage to an opponent by means of information warfare, for instance, deceiving administrative bodies or demoralizing population. It was a phenomenon associated not with an impact of Russian political class and society but rather with

installing certain ideologemes and assertion regarding our country in the Western political space. In fact, constructing the image of Russia as an “absolute destructor” waging a ‘hybrid aggression’ against the liberal world order and setting up special bodies entitled to repel it have drastically changed the way of making policy towards Russia by states and institutions of the West confined to precarious balancing between selectively cooperative approaches of traditional Russian partners in Europe and confrontational discourse promoted by new NATO and EU members from among Central and Eastern Europe. As the system of countering ‘Russian information threat’ evolved anti-Russian confrontational discourse gained a chief, guiding quality within the Western policy towards Russia. Consequently, at the moment when the Special Military Operation (SMO) in Ukraine was initiated and Russia-West confrontation reached its ‘hot stage’ the West already had at its disposal a fully operational mechanism of suppressing any positive in respect of Russia positions that allowed to disrupt in a relatively short term cooperative ties with Russia in economic, scientific and cultural dimensions despite obvious losses from such disruption for own economy and security.

For Russian diplomacy and political science emerging of such a system of information counteraction became an unexpected and quite serious challenge that should not be underestimated, ignored, or ascribed exclusively to domestic political context of certain countries in the West. However, we have to acknowledge that until recently this challenge has not received due academic attention and political response consistent with its actual meaning for pursuing national interests and foreign policy of Russian Federation. It entails the need to comprehensively study the process of launching, setting up and developing the system of countering ‘Russian information threat’ in the West in all its aspects and details and to systematize all relevant factual data for understanding the underlying mechanisms of this system and its negative effects for Russia’s status and authority in the international scene. It would, *inter alia*, pave the way to adequate assessment of current state of interaction with the West with regard to purposes of the SMO and possibilities of attaining them through negotiations.

In this research ‘Russian information threat’ does not reflect a concrete wording from the Western political rhetoric but implies a whole spectrum of actions in the information realm after 2014 that were attributed in Western media space to Russia, its government, and citizens, and were considered as a threat to own political stability and liberal democratic order. It encompasses the so called ‘Russian propaganda’, destructive intrusions of ‘Russia hackers’, bots and trolls. ‘Russia interference’ in internal political processes in Western countries and Russia’s ‘cyberwar with the free world’.

The extensive scale of phenomenon under investigation stipulated the necessity to focus upon its most meaningful, in our view, components, namely conceptual and institutional aspects of the Western system of countering ‘Russian information threat’ at its state and inter-state levels. At the same time practical aspect of its enactment and non-state arrangements employed within it fell outside the scope of this work and may become points of further research of this highly relevant and interesting problem.

**The object** of the thesis research is the Western system of countering ‘Russian information threat’ whose formation began in 2014 resulting from the so called Ukrainian crisis and subsequent events in Crimea and Donbass and whose central underlying idea is existential danger of this ‘threat’ for the whole Western liberal order.

**The subject** of the research are conceptual and institutional aspects of the Western system of countering ‘Russian information threat’, the process of their discursive formulation in academic, societal and political space in the West, their assertion as an official policy line of Western states and inter-state institutions in relevant positional documents and installation into institutional infrastructure.

**The main purpose** of the research is to reveal main actors, instruments and structures employed in the process of constructing, discursive framing and formal institutional consolidation of the Western system of countering ‘Russian information threat’, and to ascertain their respective roles in this process.

Fulfilling the main purpose required resolving the following **research tasks**:

- 1) determining when and due to what factors an image of 'Russia information threat' emerged in the Western political science;
- 2) analysis of the origin, substance and political functions of 'hybrid war' discourse as a conceptual foundation of the Western system of countering 'Russian information threat';
- 3) assessment of the idea of 'Russian information threat' as one of the central components of 'hybrid war' discourse in the Western academic and expert circles;
- 4) detecting key vectors of establishing institutional framework of information counteraction to Russia at the inter-state level in 2014-2016 period;
- 5) tracing peculiarities of initial reaction to 'Russia information threat' at the state level;
- 6) disclosing principal lines and driving forces behind improving mechanisms of countering 'Russian information threat' in the United States after election of D. Trump;
- 7) exploring the specifics of upbuilding institutional infrastructure of countering 'Russian information threat' in European countries in 2017-2019 period;
- 8) characterizing evolution of institutional arrangements of information counteraction to Russia at the inter-state level in 2017-2019 period.

**The chronologic limits** of the research include the interval from the late 2013, when during 'Euromaidan' in Ukraine there started to be voiced accusations of biased reporting of those events in some Russian media and resistance to 'pro-maidan' political shifts were regularly ascribed to 'Kremlin propaganda', up to the end of 2019. The upper chronological limit is motivated by the fact that it was the time when formation of official normative and institutional framework of system of countering 'Russian information threat' at the state and inter-state levels has been mainly completed. Later a stage of its practical employment was unleashed accompanied by abolishing certain non-state projects and structures whose functions were installed into the official institutional layout. After launching

Russian SMO in Ukraine on 24 February 2022, a new stage has started for this system with its turning into the principal generator of information stream about current events and a key factor determining political agenda and thus influencing the course of military campaign.

At the same time the research takes account of peculiarities of bringing about the image of ‘Russian information threat’ at the previous historic stage when an idea that Russia possesses some instruments of information impact and may utilize them in its foreign policy has just started to gain influence.

**Principal hypothesis** of the research. The concepts of ‘Russian information threat’, ‘information aggression’, ‘Kremlin propaganda and disinformation’ do not result from ‘voluntary’ attempts of Western academic and political circles at grasping the meaning of 2013-2014 events but are products of purposeful and well-managed ideological construction by anti-Russia forces in the West, intentionally established and eventually imposed as a political norm in order to assert the hyperbolized hostile image of Russia in the West, to hinder possible political rapprochement after the conflict potential of ‘Ukrainian crisis’ would be exhausted and to diminish agential power of Russia as international actor. These concepts provided ground for establishing a separate system of information counteraction to Russia involving non-state ‘think tanks’, representatives of academy and expertise, civil society, mass media as well as official state and inter-state structures, security services, foreign ministries, political parties and high-level officials. Portraying Russia as initiator of confrontation and pioneer in exploiting intolerable means of ‘hybrid warfare’ and ‘information aggression’ architects of these concepts managed to streamline confrontation with Russia in their preferred vein, including deploying against it the boldest instruments of deterrence. Due to constructing the system of countering ‘Russian information threat’ another dimension of confrontation with Russia has been created in the West sustained by efforts of non-state and semiofficial structures irrespective of actions or policies of Russian government *per se*.

**Theory and methodology of the research** relies on social constructivism theory that postulates in its founding provisions that political facts come about as products of social construction by political agents and gain independent meaning and impact through reification in autonomous from agential actions social structures – discursive, normative, institutional, etc. This theoretical position shaped the research prism of the thesis where ‘Russian information threat’ and its conceptual underpinning – ‘hybrid war’ discourse – are explored as products of deliberate social construction by a group of agents in the Western political space.

Proceeding from this position, central role in conducting our research was performed by process-tracing method which made possible reconstructing the course and logic of framing the system of countering ‘Russian information threat’ in the West, reveal primary sources of ‘Russian propaganda and disinformation’ discourse in 2014-2015, techniques of its dissemination, ways and driving forces of its evolution and modes of institutional reification at state and inter-state levels in subsequent years. Investigating the conceptual ground of this system was completed mainly through discourse analysis and also legal and linguistic document analysis. Incorporation and consolidation of functions on deterring and countering ‘Russian information threat’ in administrative structures of Western states and inter-state organizations was scrutinized relying on structural functional and structural institutional analysis. To contrast and compare progress of single states on the way of establishing own mechanisms of responding to ‘Russian information threat’ the research used comparative method.

It is worth noting that specifics of the research subject, which underwent further development and transformation while conducting research and also included several different levels of analysis with unobvious links between them, posed the need to find, select, assess and synthesize in a single view huge body of diverse factual data. It led to considerable expansion of thesis’s empirical base and assigning priority to techniques of systematization and generalization of information.

**The empirical base of the research.** The dissertation made use of a broad range of various sources, including:

*A) Normative base*

- official documents of NATO, the European Union and other Western inter-state institutions and of their particular bodies, among them final documents of summits, positional declarations, programmatic and strategic documents, information policy initiatives laying ground for imminence of ‘Russia information threat’ and the need to repulse it;

- official documents of particular Western states and also of their foreign and security ministries, legislative initiatives, reports and opinion directly or indirectly concerning ‘Russian information threat’ theme and mentioning admissible measures on how to counter it;

*B) Empirical base*

- public statements of Western politicians, media presentations of state officials, diplomats, oppositional leaders, public experts;

- academic publications, materials of non-state analytical ‘think tanks’, public reports on relevance of ‘Russian information threat’ and ways to neutralize it;

- propaganda web-sites, materials of media investigations, publications in media and social networks.

**The scientific novelty of the research** arises from the fact that it is the first study in Russian political science to approach the set of arrangements and instruments for constructing, affirming and countering the so called ‘Russia information threat’ shaped in the West in 2014-2019 as a single integrated complex system; to analyze its conceptual underpinning, institutional mechanisms and functions within broader context of the West-Russia confrontation. In addition, other elements of scientific novelty of the dissertation include:

- An immense amount of previously not reviewed official documents and academic papers has been introduced into Russian scientific use. Among them



seminal publications have been pointed out which imposed the frames for Western discourses on ‘hybrid war’ and ‘Russian propaganda’;

- The discourses on ‘hybrid war’ and ‘Russian information threat’ have been treated as products of social construction in Western academic and political space with their meaning lying in bundling in a single compact conventional, irregular, economic and information instruments of waging war and inter-state competition and in ascribing to Russia the role of a pioneer in exploiting these instruments for achieving military and political goals;

- System of countering ‘Russian information threat’ is represented as a disperse network construction consisting of a range of official and semiofficial bodies affiliated with the Western inter-state organizations or functioning directly within their structure and relying on a considerable non-state component embodied by various ‘think tanks’ and volunteer projects;

- Main stages in development of the Western system of countering ‘Russian information threat’ at state and inter-state levels have been proposed: the *preliminary* stage in 2006-2013 when an idea about Russia possessing significant capabilities for influencing cyberspace started circulating in the Western academic discussions; the *initial* stage in 2013-2016 when discursive grounds and institutional framework of this system at the inter-state level were laid down; and the *central* stage in 2017-2019 when key practical instruments for detecting and neutralizing ‘Russia information threat’ were introduced into administrative structures of particular states;

- Functions of system of information counteraction within broader confrontation course of the West towards Russia have been disclosed: firstly, it asserts and reifies the image of Russia as not just situational competitor but antagonist of Western values; secondly, it demonstrates how this antagonist pursues its policy beyond the limits of acceptable in sovereign states society and why the West may violate these limits in its policy towards Russia; thirdly, it sustains anti-Russia tension in the Western societies regardless of actual declarations and actions of Russian government. In such way Russia’s actorness

and authority in the international scene is artificially narrowed, its official position is deprived of legitimacy and its right to claim legal and political recognition by other states is subverted.

**Main provisions to be upheld:**

1. Unfolding of Russia-West ideational and political competition for influence on the post-Soviet societies after a series of ‘coloured revolutions’ in the middle 2000s was embraced by anti-Russian forces in the West for shaping the contours of ‘Russian information threat’. It was based on biased interpretation of Russia ascribed cyberattacks against Estonia and Georgia in 2007-2008 claimed to be a demonstration of possession by our country of capability for destructive information impact on bordering states and willingness to employ it in crises. Already at this stage among the components of such capability are mentioned not only technical skills for spurring cyberattacks but also other leverages of information impact including propaganda, activities by patriotic activists and societal groups, sympathies of Russian communities abroad.

2. ‘Hybrid war’ concept does not result from objective unprejudiced assessment of current political processes but is a product of discursive construction using expert, analytical and academic form of presenting information to impart it an image of science-based theory. It was designed to expand operative and strategic area of Russia-West confrontation including increasing the number of actual or potential participants of this confrontation, amplifying operative realms and fields and widening the diapason of acceptable instruments of combatting the opponent. ‘Hybrid war’ discourse is purported to form the hostile image of Russia as unprecedented and unconstrained danger for all liberal order, an actor pursuing illegitimate goals with intolerable means that justify similar unlimited measures of the West to turn down this threat. Mechanism of constructing this discourse consisted in massive dissemination of several key seminal publications by leading Western anti-Russian ideologists (M. Galeotti, P. Pomerantsev, M. Weiss, K. Gile, A. Illarionov, A. Polyakova, E. Lucas, M. Jaitner, P. Mattsson) which introduced core points of ‘hybrid war’ discourse and provided analytical models of their

application which later were reproduced by officials of Western states and inter-state organizations and also by political scientists. Although in academic community these points were not estimated as undisputable, the frequency of their articulation along with reification at the formal political level rendered them self-evident as objective realities not requiring supplementary proof.

3. Withing 'hybrid war' concept one the central components is an idea of 'Russian information threat' as a combination of cybernetic, networked, psychological, propaganda, disinformation, media, communicative, and other ways of impacting societal processes in the Western state or elsewhere that are employed by the Russian regime in a single global strategy with a view to subvert liberal order, discredit its values and thwart Western democratic institutions. It was set up through attributing to Russia in its origins or sources of dissemination of a whole class of widely used by Western structures social impact techniques and manipulations and of circulating in Western political space messages, narratives and ideologemes contradicting to current liberal ideological mainstream. According to this idea, Russia enjoys a considerable advantage in such modern, highly technological, innovative instruments of indirect impact while the West is still lagging in this sphere and thus remaining highly vulnerable to Russian 'hybrid' impact. Due to such merge an integrated image of destructive 'Russia propaganda and disinformation' has been erected and sustained irrespective of actual Russian position and actions in the international scene. The endpoint of constructing 'Russia information threat' amounts to delegitimizing foreign and domestic policy of Russia as a full-fledged actor in international relations with a right to assert its own position and pursue national interests by various means, including 'soft power' and public diplomacy.

4. At the initial stage of establishing system of countering 'Russian information threat' its institutional infrastructure was configured with orientation at limited scope: it was intended to cover only Russian-speaking space and countries with significant Russian communities. Leading role in this process belonged to the North Atlantic Alliance that stepped forward to become platform

for architecting discourse about Russian ‘hybrid war’ and ‘information threat’ at the official level, imposed basic guidelines for their conceptual comprehension and disseminated them through analytical materials and events by its semi-official bodies – NATO Strategic Communications Centre of Excellence in Riga and The NATO Cooperative Cyber Defence Centre of Excellence in Tallinn. Both centres were inaugurated through separate multilateral agreements of several NATO member states and were granted status of military bodies outside the Alliance integrated command after inauguration. Their organizing principles allowed to advance anti-Russia initiatives of particular NATO member states as joint position of the Alliance. Besides, NATO incorporated cyberspace and ‘hybrid threats’ into the area of its operative responsibility with a possibility to activate guarantees of Article 5 of the Washington Treaty in response to ‘hybrid attacks’ against its members.

The European Union has been getting involved into the system of countering ‘Russian information threat’ progressively starting from spring 2015 due to pressure from several member states, NATO and a number of non-state analytical institutes and ‘think tanks’. The EU concentrated on two main functions within this system, namely reacting to the challenge of ‘Russian propaganda and disinformation’ to the EU policy in the Eastern neighbourhood and forging capacity for repulsing ‘hybrid threats’ in general. The first function has been institutionalized without delay due to setup of the *East Stratcom* Task Force within the European External Action Service, the objectives of this task force being confined to detecting ‘Russian disinformation’ in the Russian-speaking information space. As regards the second function the EU has moved forward in acknowledging the relevance of information and ‘hybrid’ threats but in the basic positional documents adopted in this period (first of all, EU Global strategy of 2016) direct association of those threats with Russia has been attenuated.

Struggle with ‘Russian propaganda and disinformation’ in NATO and the EU in this period proceeded not through promoting imperative restrictive measures or waging reciprocal counter-propaganda campaigns against Russia but rather

through revealing and facts and sources of such ‘disinformation’, their timely ‘refuting’ and raising ‘awareness’ of media and ‘medialiteracy’ of society at large. In practice this approach meant regular public stigmatization of any facts and positions diverging from the Western narrative about Ukrainian crisis and subsequent events, including official position of Russian government, as false, not trustworthy and irrelevant, drawing from unverified misleading information and ‘propaganda myths’.

5. Western states joined the process of establishing the system of countering ‘Russian information threat’ in an uneven manner. At the initial stage there could be observed four types of measures resorted to by national governments: a) public discursive recognition of imminence of ‘Russian propaganda’ challenge by political leaders of certain countries, b) doctrinal reification of this challenge in positional and programmatic documents of political or, more often, strategic character, c) gathering special permanent bodies or situational working groups to tackle this challenge; d) imposing restrictive measures upon Russian media, civil society organizations or particular citizens. Several East European states (Poland, Czech Republic, and the Baltic states) rushed to introduce restrictions against Russian media and insisted on advancing this theme on the agenda of European institutions. Great Britain, Scandinavia states and the Netherlands bolstered their demands and actively participated in the newly established bodies entitled to struggle with ‘Russian propaganda’ but did not induce the initiation of such bodies at the national level. West European states came to nothing more than discursive recognition of imminence of ‘Russian propaganda’ threat or reiterating it in positional documents. In the United States, notwithstanding ample presence of discourse on ‘Russian information threat’ in the public space, practical actions in this realm did not advance far beyond fixing this threat at the parliamentary level and in military strategic thinking without making it a separate ground for initiating restrictive measures.

6. Outcomes of 2016 presidential elections in the US and resonance around putative Russian interference gave a new impetus to the process of

hammering out infrastructure for suppressing the ‘Russian information threat’ by providing an opportunity to present this threat as menacing security and stability of the West as a whole and not just of Russian-speaking space or East European countries. At this stage the necessity to counter ‘Russian propaganda’ gained legislative and institutional accommodation, with the latter embodied in three dimensions – politico-diplomatic, military and intelligence. The driving force behind this process proved to be particular intelligence and security services which joined already crystallized symbiosis of members of Congress, expertise and media with vocal anti-Russia position. They conducted public investigation of ‘Russia interference’ and put up on the agenda the need to ‘punish’ Russia for it basically through introducing sanctions mechanism specifically in the information realm and legislative approval of previously imposed sanctions to prevent their lifting by the President. Along with promulgation of Global Engagement Center within the Department of State conceived for countering foreign propaganda, the main progress was achieved in military realm owing to regular boosting of Department of Defense powers in annual National Defense Authorization Acts in respect of conducting military information operations, including preventive, clandestine and short of hostilities. Alongside constraints requiring inter-department coordination of such operations were abolished and those operation were equated with traditional military actions conducted without special coordination procedures at the level of high political authorities of the state.

7. In 2017-2019 following media resonance from presumed ‘Russian interference’ into undergoing electoral campaigns, almost all European states set about arranging their own national bodies to respond to ‘Russian information threat’. However, at this stage again they differed in types of structures promoted: in the most far-reaching cases (Great Britain, Czech Republic, Sweden) special units within security services were implanted, in other cases this threat got incorporated into strategic planning guiding documents (Belgium, Poland) and in France and Germany this process was focused on adopting legislative acts on severing control over the information realm and social networks by the national

regulating bodies. The dominant tendency in evolution of the system of suppressing 'Russian information threat' at the national level in European states consisted in legislative mandating of a new normative ground for control over information space, media and social networks with committing the latter to remove objectionable content qualified as disinformation and securing powers of state bodies to oversee its removal. This period was marked by increased role of Great Britain in architecting the infrastructure of struggle with 'Russian information threat'. Although the degree of institutionalization of functions related to the information counteraction to Russia within British state apparatus remained relatively weak, London figured as prominent generator of discourse about emanating from Russia 'hybrid threats' in the international scene, introduced rather harsh restrictions against Russian media and promoted its representatives to leading positions in international bodies created for combatting 'Russian propaganda'.

8. At the inter-state level evolution of the system of information counteraction to Russia proceeded along further incorporation and cementing information and 'hybrid' threat within strategic architecture of NATO and the EU. Political commitments on activating NATO security guarantees for repelling 'hybrid attacks' were reinforced by means of establishing within the Alliance structure of not just affiliated centres but full-fledged units responsible for monitoring, planning of operations and building capacity to be employed in case of conflicts with 'hybrid scenarios'. Also the Alliance remained the driving force behind constructing the agenda in 'hybrid threats' sphere for the European Union using among other channels the newly inaugurated European Centre of Excellence for Countering Hybrid Threats in Helsinki. Within the EU component of this system at this stage three directions can be singled out: 1) prevention and handling of challenges in cyberspace, 2) tackling the 'hybrid threats' and 3) combatting disinformation and 'fake news' with a particular importance assigned to regulating social networks. Following active engagement of the EU Commission serious progress has been achieved in setting up a separate mechanism of regulating

disinformation with concrete criteria and principles, and also responsibility of media and social networks for removal of ‘propaganda’ content.

**Theoretical value of the research** arises from the way it frames the ‘hybrid war’ concept viewing it as a special ideological construct injected into Western public and academic space rather to attain conjectural political goals in confrontation with Russia than to characterize an actual or newly discovered phenomenon. In wider context the research contributes to deepening scientific understanding about mechanisms of discursive construction of political realities in the Western public space through, inter alia, expert and academic publications of programmatic and not just descriptive character.

The results obtained therein may form the ground for further study of foreign policy of the Western states and inter-state institutions, driving forces behind shaping and implementing their policy toward Russia and post-Soviet space, including the mechanism of discursive construction of threats.

**Practical significance of the research** rests on the utility of its provisions and conclusions for appropriate and realistic formulation of aims of Russian policy towards the West under the ongoing complex political and strategic confrontation and also for acquiring due instruments of sustaining own international image and information security. Besides, they may be of use in a range of studying courses related to Russia’s foreign policy, current international processes, conflict studies and information security.

**The field of thesis research** corresponds to paragraph 2 “Actors in international relations. Activities of state and non-state actors. Formal and informal institutions in international relations and world politics. Formulation and implementation of foreign policy strategies, conceptions and doctrines”; and paragraph 17 “Information, cognitive, bio- and other new technologies in international relations and world politics” of the passport of specialty 5.5.4. ‘International relations, global and regional studies’.

**Approbation of the research results.** Main provisions and conclusions of the research were presented at several scientific conferences: XVII International



scientific and practical conference ‘Relevant issues in modern science’ (Tomsk, 19 December 2018); XII International scientific and practical conference ‘Relevant issues in science and practice’ (Samara, 10 December 2018).

Principal research results presented in the dissertation of V. S. Tsarik have been captured in 8 academic publications with cumulative scope of 5,8 p.l., including 4 scientific articles in journals recommended by the Higher Attestation Commission under the Ministry of Science and Higher Education of the Russian Federation and included in the List of editions approved by the Academic Council of Russian Presidential Academy of National Economy and Public Administration of 17 April 2018:

**A. Articles in editions included in the List of leading peer-reviewed journals recommended by the Higher Attestation Commission under the Ministry of Science and Higher Education of the Russian Federation:**

1. Tsarik V. S. The “hybrid war” constructing in Western media space.. Main stages and actors / V. S. Tsarik // RSUH/RGGU Bulletin. “Political Science. History. International Relations” Series. – 2020. –No. 3. – P. 20-34. (0,9 p.l.)

**B. Articles in editions recommended by the Academic Council of Russian Presidential Academy of National Economy and Public Administration:**

2. Tsarik V. S. System of Counteraction to "Russian Information Threat" in the West: Structure, Basic Levels and Tools / V. S. Tsarik // Middle Russian Review of social science. – 2018. – Vol. 13. – No. 6. – P. 97-110. (0,7 p.l.)

3. Tsarik V. S. Fighting against ‘Russian Disinformation’ in Public Positioning of Western Institutions: Analysis of Official Sites of NATO and the European Union / V. S. Tsarik // Middle Russian Review of social science. – 2019. – Vol. 14. – No. 6. – P. 109-125. (1 p.l.)

4. Tsarik V. S. Countering ‘Russian Information Threat’ in the European Union Policy after the Ukraine Crisis: Discourse and Institutional Aspects / V. S. Tsarik // Middle Russian Review of social science. – 2020. – Vol. 15. – No. 5. – P. 107-123. (0,9 p.l.)

### C. Other publications:

5. Tsarik V. S. Western interpretation of information conflicts around Estonia and Georgia in 2007-2008 in context of 'hybrid war' concept / V. S. Tsarik // Relevant issues in modern science: collection of articles reflecting materials of XVII International scientific and practical conference. – Ufa: Dendra, 2018. – P. 173-182. (0,5 p.l.)

6. Tsarik V. S. Main approaches to researching 'hybrid war' in Russian political science / V. S. Tsarik // Relevant issues in science and practice: collection of articles reflecting materials of XIII International scientific and practical conference. – Ufa: Dendra, 2018. – P. 161-171. (0,5 p.l.)

7. Tsarik V. S. Activity of Western Non-Governmental Organizations and Analytical Institutes in Countering 'Russian Disinformation' / V. S. Tsarik // Bulletin of International Institute of Law. – 2019. – No. 4 (71). – P. 152-165. (0,7 p.l.)

8. Tsarik V. S. Stage-by-Stage Principle in Restricting Regulation of Information Space in Response to 'Russian Information Threat' (Basing on Germany and France Examples) / V. S. Tsarik // Bulletin of International Institute of Law. – 2020. – No. 3 (74). – P. 14-27. (0,6 p.l.)

**Thesis structure** is conditioned by the research purpose and tasks. The dissertation scope complies with the requirements of the Higher Attestation Commission under the Ministry of Science and Higher Education of the Russian Federation and consists of introduction, three chapters, eight paragraphs, and bibliographic list.



/V. S. Tsarik /