APPLIED ANALYSIS

ПРИКЛАДНОЙ АНАЛИЗ

DOI: 10.22363/2313-0660-2025-25-3-469-484
EDN: WNKTNS

Research article / Научная статья

ICT Security in U.S. Foreign Policy Towards Latin America: The Case of the Biden Administration's Discourse

Lev M. Sokolshchik[1] ✉, **Inna O. Yanikeeva**[1], **Gleb V. Toropchin**[2,3]

[1]National Research University Higher School of Economics, Moscow, Russian Federation
[2]Novosibirsk State Technical University, Novosibirsk, Russian Federation
[3]National Research Tomsk State University, Tomsk, Russian Federation
✉ lsokolshchik@hse.ru

Abstract. The issue of information and communication technology (ICT) security is becoming increasingly important in the context of international relations and foreign policy. In the present study, the authors analyze the discourse of the Joseph Biden administration in the field of international ICT security in the Latin American dimension, with the aim of identifying the underlying ideology that supports and justifies the U.S. power relations with the region. The scientific novelty of the present study lies in the integrated application of the critical discourse analysis (CDA) method, which allows examining how language practices shape ICT security perceptions and political reality. In addition, the study employs quantitative content analysis, which provides insights into attributed threats, primarily among state actors. The authors conduct the CDA at the contextual and discursive levels. The study's extensive source base includes materials from U.S. government agencies, encompassing the period from January 2021 to November 2024. The authors critically examine the image of the United States as an agent constructing international ICT security in the Latin American dimension from the perspective of its hegemonic aspirations. The image of Latin America as a region vulnerable in the ICT space and in need of paternalism from Washington is a significant element of the U.S. discourse. At the same time, the images of China and Russia are presented as the main sources of threat to the region to justify the dominant role of the United States. In the background of American discourse, the Democratic People's Republic of Korea (DPRK) and the Islamic Republic of Iran (IRI) are presented as limited but growing threats to ICT security. These discursive practices serve as a tool to legitimize American influence and promote its strategic interests in the region.

Key words: information security, cybersecurity, critical discourse analysis, content analysis, China, Russia, Iran, the Democratic People's Republic of Korea, the DPRK

Conflicts of interest. The authors declare no conflicts of interest.
Authors' contributions. L.M. Sokolshchik: conceptualization, development of methodology and research design, scientific supervision, writing — preparation of a draft manuscript, scientific editing. I.O. Yanikeeva: data collection and processing, qualitative analysis, writing — preparation of a draft manuscript, manuscript design. G.V. Toropchin: data processing, quantitative analysis, visualization, writing — preparation of a draft manuscript. All authors have read and approved the final version of the article.

Acknowledgements. The research was supported by RSF (project No. 22-78-10014, https://rscf.ru/project/22-78-10014/).

For citation: Sokolshchik, L. M., Yanikeeva, I. O., & Toropchin, G. V. (2025). ICT security in U.S. foreign policy towards Latin America: The case of the Biden administration's discourse. *Vestnik RUDN. International Relations*, 25(3), 469–484. https://doi.org/10.22363/2313-0660-2025-25-3-469-484

ИКТ-безопасность во внешней политике США в отношении Латинской Америки: кейс дискурса администрации Дж. Байдена

Л.М. Сокольщик[1] ✉, **И.О. Яникеева**[1], **Г.В. Торопчин**[2,3]

[1]Национальный исследовательский университет «Высшая школа экономики», Москва, Российская Федерация
[2]Новосибирский государственный технический университет, Новосибирск, Российская Федерация
[3]Национальный исследовательский Томский государственный университет, Томск, Российская Федерация
✉ lsokolshchik@hse.ru

Аннотация. Проблема безопасности в сфере информационно-коммуникационных технологий (ИКТ) приобретает все возрастающее значение в контексте международных отношений и внешней политики. Исследование посвящено анализу дискурса администрации Дж. Байдена в области международной ИКТ-безопасности на латиноамериканском направлении. Цель — выявление скрытой в дискурсе идеологии, поддерживающей и оправдывающей властные отношения США со странами Латинской Америки. Научная новизна работы состоит в комплексном применении метода критического дискурс-анализа (КДА), позволяющего рассмотреть, как языковые практики формируют восприятие ИКТ-безопасности и политической реальности, а также количественного контент-анализа, дающего представление об атрибутируемых угрозах, в первую очередь среди государственных акторов, что ранее не получило должного внимания в научной литературе. КДА проводится на контекстуальном и дискурсивном уровнях. Исследование опирается на широкую источниковую базу, включающую материалы государственных органов США за период с января 2021 по ноябрь 2024 г. Авторы критически осмысляют образ США как агента, конструирующего международную ИКТ-безопасность на латиноамериканском направлении, в ракурсе своих гегемонистских устремлений. Выявлено, что значимым элементом американского дискурса является образ Латинской Америки как региона, уязвимого в ИКТ-пространстве и нуждающегося в патернализме со стороны Вашингтона. Образы Китая и России представляются как основные источники угроз в регионе для оправдания доминирующей роли США. На втором плане американского дискурса присутствуют образы Корейской Народно-Демократической Республики (КНДР) и Исламской Республики Иран (ИРИ), которые позиционируются как ограниченные, но растущие угрозы в ИКТ-пространстве. Авторы приходят к выводу, что подобные дискурсивные практики служат инструментом легитимации влияния США и продвижения ими своих стратегических интересов в регионе.

Ключевые слова: информационная безопасность, кибербезопасность, критический дискурс-анализ, контент-анализ, Китай, Россия, Иран, Корейская Народно-Демократическая Республика, КНДР

Заявление о конфликте интересов. Авторы заявляют об отсутствии конфликта интересов.

Вклад авторов. Сокольщик Л.М.: концептуализация, разработка методологии и дизайна исследования, научное руководство, написание — подготовка черновика рукописи, научное редактирование. Яникеева И.О.: сбор и обработка данных, проведение качественного анализа, написание — подготовка черновика рукописи, оформление рукописи. Торопчин Г.В.: обработка данных, проведение количественного анализа, визуализация, написание — подготовка черновика рукописи. Все авторы ознакомлены с окончательной версией статьи и одобрили ее.

Благодарности. Исследование выполнено за счет гранта Российского научного фонда № 22-78-10014, https:// rscf.ru/project/22-78-10014

Для цитирования: *Сокольщик Л. М., Яникеева И. О., Торопчин Г. В.* ИКТ-безопасность во внешней политике США в отношении Латинской Америки: кейс дискурса администрации Дж. Байдена // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2025. Т. 25, № 3. С. 469–484. https://doi.org/10.22363/2313-0660-2025-25-3-469-484

Introduction

In recent decades, the issue of security in the field of information and communication technologies (ICT) has become an integral part of the political agenda at both international and national levels. There has been growing interest in this topic within the scientific community (Krutskikh, 2022; Ponka, Ramich & Wu, 2020; Bolgov, 2020; Henshaw, 2024; Hurel, 2022). At the same time, countries at the United Nations (UN) level recognize that ICT issues are becoming increasingly politicized.[1] The desire to ensure security in this sphere often conceals the hegemonic aspirations of international actors. U.S. foreign policy towards Latin America under the Biden administration is one example of this.

There is no single conceptual framework describing this area of research in the scientific literature. Several approaches exist to understanding security in the ICT sphere. A broad interpretation covers information security, incorporating all aspects of security in the digital environment, including political aspects. In contrast, a narrower interpretation implies that cybersecurity encompasses the technical aspects of preventing threats and risks to digital infrastructure, software and hardware (Zinovieva & Ignatov, 2023, pp. 107–108).

The concepts of “cybersecurity” and “information security” are often confused and used as synonyms. In this regard, the analytical category of “ICT security” is employed in our research as a compromise term that includes the entire spectrum of security issues in the area under consideration (Zinovieva & Ignatov, 2023, pp. 107–108) and implies countering threats in the ICT sphere, as well as threats arising from the use of ICT in the military-political, ideological-political, social, economic, infrastructural and technological contexts.

Although Washington officially adheres to the interpretation of ICT security within the concept of “cybersecurity,” the American discourse covers elements of a broader concept of information security, including fighting cyberterrorism, disinformation campaigns and information interference in a state’s internal affairs.[2] In this regard, using the broader term of “ICT security” in relation to the American case seems more than justified.

The U.S. plays an important role in the world’s digital transformation. It stood at the origin of the Internet. It is currently actively using its potential in the ICT sphere to achieve foreign policy goals. Discursive practices, defined as systematic and planned speech acts by political agents (Sokolshchik, Sokolshchik & Teremetskiy, 2024, p. 113), represent a means through which power relations are established. The issue of ICT security is seldom addressed in a discursive capacity, mainly due to their practical significance for foreign policy. Our aim is to address this shortcoming by conducting comprehensive research into the discourse surrounding ICT security during the Biden administration within the context of U.S. foreign policy in Latin America.

The discourse on ICT security in official U.S. materials reflects Washington’s international ambitions in the context of the transformation of the international order. Following the proclamation of the Monroe Doctrine in the first quarter of the 19th century,

[1] Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: Note by the Secretary-General (A/76/135) // UN. July 14, 2021. URL: https://docs.un.org/en/A/76/135 (accessed: 15.01.2025).

[2] United States International Cyberspace & Digital Policy Strategy // U.S. Department of State. May 6, 2024. URL: https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf (accessed: 15.01.2025).

Latin America has become one of the priority regions for U.S. foreign policy. It is natural that the region occupies one of the central places in the discourse under consideration. At the same time, from the U.S. perspective, Latin America is highly vulnerable in the ICT sphere and therefore in need of paternalism from Washington.

In our research, the term ‘Latin America’ is employed to denote the entire continent of South America, including Mexico, the countries of Central America and the Caribbean islands, whose inhabitants speak Romance languages (Sokolshchik, Sakaev & Galimullin, 2023, p. 108).

The basic premise of the research is predicated on several constructivist principles. First of all, political reality does not exist by itself. Its meaning is a product of social construction and the interpretations of various agents (Campbell, 1993) pursuing political goals (Krebs, 2015, p. 810). These agents create a subjective world of politics, which is not identical to objective reality, although it may have referents (Sokolshchik, Sokolshchik & Teremetskiy, 2024, p. 111; Sokolshchik, 2024). States, as the principal agents on the world stage, mutually recognize the right of sovereignty through communicative interaction, thereby legitimizing each other’s existence and forming a system of international relations (Wendt, 1999, pp. 10–11). Agents construct political being by creating discourses that not only reflect political relations but also significantly influence them (Miao, Xu & Zhu, 2019, p. 2).

In the context of the research, the process of securitization (Buzan, Wæver & de Wilde, 1998) is of great importance as a discursive practice (Sokolshchik & Sokolshchik, 2023), in which the *agent* designates a certain *object* as a security threat and provides the *recipient* with arguments in favor of countermeasures against the securitized object (Miao, Xu & Zhu, 2019, p. 2).

The present research aims to analyze the hidden ideology in the U.S. ICT security discourse in the Latin American dimension, which supports and justifies the power relations between Washington and the states of the region.

The ICT security discourse is analyzed as a complex of fears and threats at the global and national levels (Tikk & Kerttunen, 2020). In terms of country cases, the content analysis method is applied to doctrinal documents on ICT security in several Latin American countries, including Argentina, Brazil, Chile, Colombia, Mexico, Peru (Urbanovics, 2022). R. Siudak identifies two main types of the ICT security discourse in terms of their influence on policy: technical discourse and the discourse of national security (Siudak, 2022). I. Stadnik (2024) explores the potential of critical discourse analysis (CDA) by examining the bilateral relations between the United States and Russia in the ICT security sphere. Overall, studies that explore the discursive construction of ICT security and critically analyze its structures remain fragmented.

The Methodological and Source Base of the Study

The methodological framework of the research includes the CDA in combination with the quantitative content analysis. The CDA implies identifying a hidden ideology in an *agent’s* speech that supports social power, dominance and inequality. The starting point for CDA is the assumption that the *agent* imposes on the *recipient* a certain figurative or symbolic order as the exclusively correct one through discourse (Pakhalyuk, 2018, p. 165). From this perspective, discourse is understood as a political act and a means of reproducing power.

The research focuses on the pragmatic aspect of discourse (Fomin, 2014a, p. 129) as it relates to a specific part of the socio-political reality or a “field of action” (Reisigl & Wodak, 2009, pp. 90–91). The agent construct this “field” through *cognitive models* that set the context for discourse (van Dijk, 2006, p. 163), reflecting the connections between personal knowledge of events, on the one hand, and shared beliefs in society, on the other. As T. van Dijk (2006, pp. 168–170) observes, cognitive models of context form the basis of the "pragmatic" interpretation of discourse, since their structure determines its implementation and understanding.

Considering the specifics of the research subject, the "field of action" in the research is defined as the cognitive model of the international ICT space constructed by the U.S., thereby providing the context for a specific discourse on ICT security in the Latin American dimension. Within the framework of the cognitive model of the international ICT space of the U.S., we have identified the following structural elements: *global* and *regional dimensions*, as well as *ICT threats* and the *methods/tools to counter them*.

In the sphere of communicative interaction, hidden ideology is implemented through constructed images of the *agent, recipient*, and the *objects* of securitization (Fomin, 2014b, p. 51). In this case, an image is defined as "a semiotic construction formed within the framework of a specific discourse and accumulating acts of comprehension and signification characteristic of this discourse" (Svirchevskii & Fomin, 2023, p. 29). The creation of these images is facilitated by discursive strategies, which can be defined as the agent's intentionally implemented plans to use language to achieve political goals (Fomin, 2014a, p. 129).

The following discursive strategies are identified: *referential* (construction of phenomena, actors, processes), *predicational* (attribution of positive or negative characteristics to phenomena, actors, processes), and *an argumentation system* (justification / challenge of theses).

Thus, we conduct the CDA at two levels: firstly, the contextual level ("field of action") — through analyzing the *American mental model of the international ICT space* as the context of the discourse under consideration; and, secondly, the discursive level — through analyzing the images of the *agent* (the U.S.), the *recipient* (Latin America) and the *objects of securitization*, which are created through discursive *referential* and *predicational* strategies, as well as an *argumentation system* in favor of the constructed image system.

Quantitative content analysis complements qualitative analysis. It is used to analyze the frequency of references to objects as threats and proposed policy solutions in a corpus of sources. To conduct the content analysis, we used *QDA Miner Lite*[3] software to analyze the corpus of U.S. foreign policy documents loaded into the app, in order to determine the frequency with which state actors were referenced as objects of securitization and the threats attributed to them.

The research is based on materials from the official websites of U.S. government agencies, including the White House, the State Department, the Department of Defense, the Department of Justice, and the Department of Homeland Security. The chronological framework covers the period from January 20, 2021 (the inauguration of President Joseph Biden) to November 13, 2024 (the most recent data available at the time of writing the research paper).

The data collection was carried out in three stages. Initially, a search was conducted using the token "*Latin America*." Then, we extracted from the resulting array documents containing the lexemes "*cyber,*" "*digital,*" "*artificial intelligence*." At the final stage, we carried out a selection of documents directly related to the topic of ICT security by searching for the token "*security*." Thus, 47 documents were selected for analysis.[4] The main data array was supplemented

[3] QDA Miner // Provalis Research. URL: https://provalisresearch.com/products/qualitative-data-analysis-software/freeware/ (accessed: 25.12.2024).

[4] Among them, for example, see: 2022 National Defense Strategy of the United States of America // U.S. Department of Defense. October 27, 2022. URL: https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF (accessed: 15.01.2025); National Security Strategy // The White House. October 2022. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (accessed: 15.01.2025); United States International Cyberspace & Digital Policy Strategy // U.S. Department of State. May 6, 2024.

with materials from the media, international organizations, international projects in the ICT security sphere, and think tanks.

The Cognitive Model of the International ICT Space

Global Dimension

In the context of American political discourse, it is argued that the international system is in crisis. The era of global development that began after the collapse of the bipolar system is coming to an end. Great-power rivalry for influence in key regions, including Latin America, and in various areas, including ICT, is coming to the forefront of international relations. In this regard, American official documents and statements emphasize the need to maintain the country's dominance on the world stage. Leadership in ICT, the digital economy, and new technologies is considered essential for advancing U.S. interests. It is also argued that U.S. primacy in the ICT sphere not only strengthens the country's national security but also supports democratic values and contributes to "improving the lives around the world."[5]

The American concept of the ICT space places particular emphasis on the institutional aspect, international norms and cooperation. It is claimed that the United States, together with its partners, seeks to strengthen multilateral institutions, particularly the UN, to improve the rules of interaction in this area. At the same time, it is emphasized that international norms must be "fair" to American workers and corporations, protecting "competition" and maintaining U.S. economic and technological superiority.[6] Thus, the global institutional structure of the ICT space, in Washington's view, should support the dominant position of the United States in the global economy and politics.

It is argued that opponents of the U.S. seek to use international institutions to achieve goals that are contrary to American interests.[7] The U.S. characterizes Russia and China as countries that use multilateral institutions, including the UN, to exert influence over developing countries and to attempt to change norms in the ICT space. At the same time, the world is divided along the ideological antithesis of "democracy vs. autocracy." This discourse aims to create the impression that digitalization benefits states only if Washington leads the process.

With U.S. interests constrained in the UN Security Council by the veto power of China and Russia, Washington is trying to replace universal institutions with "democracy summits."[8] Through these forums, the U.S. sought to present its ICT agenda as the opinion of the "international community". For instance, the 2023 and 2024 summits, among other details, emphasized the commitment of participating countries to the development of "emerging technologies to align with democratic values and human rights."[9] Moreover, the main criterion for the "democratic" nature of a particular country is its partnership with the United

URL: https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf (accessed: 15.01.2025); National Cybersecurity Strategy // The White House. March 2, 2023. URL: https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/ (accessed: 15.01.2025).

[5] Joint Strategic Plan FY 2022–2026 // U.S. Department of State. March 2022. URL: https://www.state.gov/wp-content/uploads/2022/03/Final-State-USAID-FY-2022-2026-Joint-Strategic-Plan_29MAR2022.pdf (accessed: 15.01.2025).

[6] National Security Strategy // The White House. October 2022. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (accessed: 15.01.2025).

[7] United States International Cyberspace & Digital Policy Strategy // U.S. Department of State. May 6, 2024. URL: https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf (accessed: 15.01.2025).

[8] Summit for Democracy. URL: https://summit4democracy.org/ (accessed: 15.01.2025).

[9] 2024 Report on the Cybersecurity Posture of the United States // The White House. May 2024. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf (accessed: 15.01.2025).

States. Thus, the U.S. discriminatory discourse is justified by making distinctions between "friend or foe" (Sokolshchik, Sakaev & Galimullin, 2023, p. 119).

Regional Dimension

To successfully implement the ICT agenda at the regional level, the Biden administration has sought to use multilateral forums such as the Organization of American States (OAS). Established at the dawn of the Cold War under the auspices of the United States, the OAS united all the states of North and South America, except Cuba, and became the core of the inter-American system of international relations (Kheifets & Khadorich, 2015, p. 94). The organization remained largely a conduit for U.S. interests even after the end of the bipolar confrontation (Kheifets & Khadorich, 2015, pp. 94–96). The discourse under consideration emphasizes that the United States supports the OAS efforts in areas such as ICT incident response, ICT security awareness, and ICT security training. At the same time, since 2003, the OAS has been implementing the Cybersecurity Program, which aims to form a conceptual basis for the national strategies of member states in this area.[10]

In addition, the OAS is a collective member of international ICT security platforms operating under the auspices of the United States, including the International Counter Ransomware Initiative[11] and the Global Forum on Cyber Expertise.[12] A number of Latin American countries independently participate in U.S.-led ICT security initiatives and partnerships, such as the Declaration for the Future of the Internet (Argentina, Colombia, Costa Rica, Peru, Trinidad and Tobago, Uruguay)[13] and the Freedom Online Coalition (Argentina, Chile, Colombia, Costa Rica, Mexico).[14] Relying on the OAS and other multilateral institutions allows for greater coordination in advancing the American agenda at the regional level and presents the United States as a provider of "collective" ICT security. Moreover, the United States is actively developing cooperation on a bilateral basis, interacting with almost all countries in the region.

Threats in the ICT Space

In the American discourse, four broad areas can be identified where ICT threats manifest themselves, which generally correspond to the classification of the U.S. Department of Homeland Security[15]:

1) public safety (e.g., disinformation, cyberterrorism, election interference),

2) border and migration security (e.g., transnational criminal organizations),

3) critical infrastructure security (e.g., cyberattacks and cyberespionage against energy and transport facilities),

4) economic security (e.g., cyberattacks and cyberespionage for financial purposes, market manipulation).

These areas are all important to consider when discussing ICT threats in the United States.

The U.S. officials state that international conflicts are increasingly unfolding in the ICT space, escalating the risks to the security of the U.S. and its allies.[16] Among the state actors that

[10] Cybersecurity Program // OAS. 2003. URL: https://www.oas.org/ext/en/security/prog-cyber (accessed: 15.01.2025).

[11] International Counter Ransomware Initiative 2024 Joint Statement // The White House. October 2, 2024. URL: https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/10/02/international-counter-ransomware-initiative-2024-joint-statement/ (accessed: 15.01.2025).

[12] GFCE. URL: https://thegfce.org/ (accessed: 15.01.2025).

[13] A Declaration for the Future of the Internet // The White House. April 28, 2022. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf (accessed: 15.01.2025).

[14] Freedom Online Coalition. URL: https://freedomonlinecoalition.com/ (accessed: 15.01.2025).

[15] Homeland Threat Assessment 2024 // Homeland Security. URL: https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf (accessed: 15.01.2025).

[16] 2024 Report on the Cybersecurity Posture of the United States // The White House. May 2024. URL:

the United States perceives as key threats in the ICT sphere, China and Russia stand out first and foremost. The list is supplemented by the Democratic People's Republic of Korea (DPRK) and the Islamic Republic of Iran (IRI).

The American discourse also contains a description of the following methods/tools for countering ICT threats:

– strengthening alliances and partnerships in the ICT sphere (collective cyber defense),

– expanding activities based on international organizations and institutions,

– developing international norms and rules in the ICT sphere, including in the field of artificial intelligence (AI),

– establishing international law enforcement mechanisms in the ICT space,

– ideologizing the ICT security agenda by dividing the world according to the "friend or foe" principle,

– expanding the U.S. presence abroad, including intelligence agents,

– strengthening controls over the export and distribution of advanced ICT and components,

– investments in the national IT industry, including AI, 5G and 6G, cloud infrastructure, and data centers,

– provision of international assistance for the development in the ICT sphere, including training specialists,

– application of sanctions to ensure national interests and security in the ICT space.

Hidden Ideology in the U.S. Discourse

The Image of an Agent

The United States, as an agent of the discursive process, seeks to promote its idea of ICT security on the international stage as exclusive and true. Washington positions itself as a "defender of freedom and democracy," a "leader in technology," and a "security partner," emphasizing its unique role in countering ICT threats and its commitment to cooperation. It is postulated that the U.S. should play a leading role in shaping global norms and institutions in the ICT sphere, especially in the field of AI. The American discourse argues that the United States has been a world leader throughout its history in developing advanced technologies, which it has used not only for strengthening national security but also for promoting democracy around the world.[17]

The United States often tends to overstate its positive qualities and hide its desire for dominance in Latin America. The U.S. activities in the field of ICT security are presented as an exceptional benefit for the region, as it seeks to strengthen the ICT capacity of Latin American countries to protect human rights and democracy, economic and technological development, and to strengthen sovereignty. In this interpretation, the successful development of Latin American countries is only possible with the use of American technological solutions, since only they can provide a "secure digital infrastructure." Therefore, the U.S. forms an image of itself as an indispensable "provider" of ICT security for Latin American countries.

Recipient Image

As previously noted, the U.S. considers Latin America to be a region with a high level of vulnerability in the ICT space, which requires paternalism. On the one hand, this justifies the humiliated and predominantly passive position of Latin American states, and, on the other hand, it allows for the leading and a priori active role of the United States in the region. Given the

https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf (accessed: 15.01.2025).

[17] Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence // The White House. October 24, 2024. URL: https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/ (accessed: 15.01.2025).

importance of a multilateral approach that is often used in the American hegemonic discourse, the United States acknowledges that Latin American countries “contribute to collective efforts to develop cyberspace.”[18]

The U.S. officials describe the Western Hemisphere as a community of like-minded nations to convince the recipient of the need for joint action in the ICT sphere, as the U.S. sees it. Behind the American theses lies the intention to convince Latin America of the importance of choosing Washington as a partner in the digital environment, rather than someone “foreign.” The discourse is reinforced by statements that the U.S. prioritizes the presence of “reliable suppliers” of ICT security in the region, which can only be ensured by Washington.

From the U.S. perspective, Latin American countries incapable of achieving independent development in the ICT sphere. The model of unequal relations is implicit in almost all aspects of the discourse under consideration, including the issue of development assistance. The U.S. discourse emphasizes the low technological level of the countries in the region and the vast opportunities for the United States to assist their development in this area. It is suggested that Latin American countries need to make a “choice between investing in the digital future or in renewable energy,”[19] while the U.S. stands ready to invest resources in the region to support its digital development, including 5G infrastructure.

Images of Securitization Objects

In the American ICT security discourse, China and Russia are identified as the main threats causing destabilization for the Latin American region. Beijing is described as a “strategic competitor with the capacity to threaten U.S. interests and dominate emerging technologies.” Meanwhile, Moscow is presented as a “persistent cyber threat as it refines its capabilities” to weaken the alliances and partnerships of the United States.[20] At the same time, it is stated that Latin American countries are concerned about the possibility of disinformation from Russia: “[The United States] provided technical assistance and support to try to ensure that Colombian institutions are able to defend their infrastructure and to push back on [Russian] disinformation.”[21] China is portrayed as a more serious threat to the United States and Latin American countries, since Beijing seeks to surpass Washington in the ICT sphere and offers comprehensive development solutions in this area. The image of China is formed as a systemic threat to the United States across the entire spectrum of ICT security issues. Thus, in the American discourse it is postulated that “over the last ten years, it has expanded cyber operations … to become our most advanced strategic competitor with the capacity to threaten U.S. interests and dominate emerging technologies.”[22] In turn, Russia, according to the United States, is gradually increasing its ICT potential to expand “malicious” activity against the United States, including in Latin America. Russia is said to be seeking to maintain its influence in the Western Hemisphere by developing cooperation with a select group of

[18] Remarks: National Cyber Director Coker at LATAM CISO // The White House. September 13, 2024. URL: https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/09/13/remarks-national-cyber-director-coker-at-latam-ciso/ (accessed: 15.01.2025).

[19] Remarks by President Biden at the Fourth CEO Summit of the Americas // The White House. June 9, 2022. URL: https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2022/06/09/remarks-by-president-biden-at-the-fourth-ceo-summit-of-the-americas/ (accessed: 15.01.2025).

[20] National Cybersecurity Strategy // The White House. March 2, 2023. URL: https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/ (accessed: 15.01.2025).

[21] Background Press Call by Senior Administration Officials Previewing the Visit of President Duque of Colombia // The White House. March 9, 2022. URL: https://bidenwhitehouse.archives.gov/briefing-room/press-briefings/2022/03/10/background-press-call-by-senior-administration-officials-previewing-the-visit-of-president-duque-of-colombia/ (accessed: 15.01.2025).

[22] National Cybersecurity Strategy // The White House. March 2, 2023. URL: https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/ (accessed: 15.01.2025).

countries: Argentina, Brazil, Venezuela, Cuba, and Nicaragua.[23]

In the background of the American discourse are the DPRK and Iran, posing a limited threat, but are increasing the scale of their "malicious activity" in the ICT sphere.[24] Iran "uses cyber capabilities to threaten U.S. allies," while the DPRK "generates revenue through criminal enterprises" using ICT.[25] It is argued that further development of these countries' ICT capabilities could seriously impact the security of the United States and its partners.[26]

Thus, in the U.S. discourse, the most significant threats in the ICT sphere are clearly those powers that can offer Latin American countries an alternative development path to that offered by the U.S., that are primarily China and Russia.

Argumentation System

In order to legitimize the "agent-recipient-object" system (Table 1), the United States employs a variety of arguments. It seeks to justify its special role in Latin America by promoting the idea of shared security and emphasizing the need for collective action. This enables it to coordinate multilateral efforts in the ICT security sphere. The partnerships formed with Latin American countries are argued to be crucial for forming a shared vision of cyberspace. Arguments are given about the close economic ties and shared values of North and South American countries. The U.S. actively employs ideologically charged arguments. Thus, it is postulated that "countries that use digital tools and technology responsibly — respecting human rights and democratic values — are stronger when we work together."[27] At the same time, it is implicitly assumed that joint actions should be carried out with the leading role of the United States.

Washington uses hypothetical scenarios, such as the possible collapse of critical infrastructure and large-scale cyberattacks, to justify the need for its presence in the region. At the same time, the rhetoric of altruism can be traced in the American discourse. U.S. policy is presented as aimed solely at protecting human rights and democratic institutions. Indeed, the United States provides extensive technical and expert assistance to Latin American countries in developing ICT security strategies, establishing incident response centers, strengthening infrastructure, and combating international ICT-enabled crime.[28] It often presents the aid policy as an expression of U.S. "goodwill." At the same time, hidden strategic goals, such as strengthening economic and political influence in the region, remain implicit.

[23] Annual Threat Assessment of the U.S. Intelligence Community // Office of the Director of National Intelligence. February 6, 2023. URL: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf (accessed: 15.01.2025).

[24] United States International Cyberspace & Digital Policy Strategy // U.S. Department of State. May 6, 2024. URL: https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf (accessed: 15.01.2025).

[25] National Cybersecurity Strategy // The White House. March 2, 2023. URL: https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/ (accessed: 15.01.2025).

[26] Ibid.

[27] Remarks: National Cyber Director Coker at Singapore International Cyber Week 2024 // The White House. October 15, 2024. URL: https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/10/15/remarks-national-cyber-director-coker-at-singapore-international-cyber-week-2024/ (accessed: 15.01.2025).

[28] See: Fact Sheet: Advancing Technology for Democracy // The White House. March 29, 2023. URL: https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/03/29/fact-sheet-advancing-technology-for-democracy-at-home-and-abroad/ (accessed: 15.01.2025); Digital Connectivity and Cybersecurity Partnership (DCCP) // Cybil. URL: https://cybilportal.org/projects/digital-connectivity-and-cybersecurity-partnership-dccp/ (accessed: 15.01.2025); Joint Statement on the U.S. — Chile High-Level Dialogue // U.S. Embassy in Chile. October 2, 2024. URL: https://cl.usembassy.gov/joint-statement-on-the-u-s-chile-high-level-dialogue/#:~:text=During%20the%20HLD%2C%20the%20United,cybercrime%2C%20and%20emerging%20threats%3B%20and (accessed: 15.01.2025).

Table 1. **The Image System in the U.S. ICT Security Discourse**

Image	**Referential strategies**	**Predicational strategies**
The USA as an *agent*	– Global leader in ICT – Defender of freedom and democracy – Arbiter in the ICT space – Most attractive partner in the ICT space – Reliable provider of ICT security	– Pursues policies to preserve the rules-based world order – Defends liberal values – Sets international norms in the ICT space – Uses ICT for "good" purposes – Is interested in cooperation – Intends to help partners – Seeks to strengthen multilateral institutions – Seeks to ensure fair competition considering its interests – Seeks to ensure collective security
Latin America as a *recipient*	– Region with a high level of vulnerability in the ICT space – Region with a low level of ICT development – Region dependent on external assistance – Predominantly passive partner	– Needs U.S. paternalism – Needs assistance to ensure ICT security – Needs resources for ICT development – Contributes to collective ICT security
China as an *object of securitization*	– Non-liberal state – Strategic competitor – Most serious threat to the U.S. and Latin America – Systemic threat – Source of destabilization in politics, economics, the ICT space	– Conducts revisionist foreign policy – Seeks to surpass the U.S. in the ICT space – Promotes digital authoritarianism – Uses ICT to achieve aggressive foreign policy goals – Undermines international norms – Is capable of carrying out serious cyber-attacks – Violates human rights using ICT
Russia as an *object of securitization*	– Non-liberal state – Tactical competitor – Significant threat to U.S. interests in certain Latin American countries – Source of destabilization in politics, economics, the ICT space	– Conducts revisionist policy – Improves ICT capabilities to expand malign activities against the USA and its allies – Carries out disinformation and propaganda – Uses ICT to achieve aggressive foreign policy goals – Undermines international norms in the ICT space – Violates human rights using ICT
The DPRK as an *object of securitization*	– Non-liberal state – Limited threat to the USA and its allies, including Latin American countries – Source of destabilization in politics, economics, the ICT space	– Conducts revisionist policy – Expands the scope of malicious activity in the ICT space – Uses ICT to achieve aggressive foreign policy goals – Receives income from criminal activity using ICT – Violates human rights using ICT
Iran as an *object of securitization*	– Non-liberal state – Limited threat to the USA and its allies, including Latin American countries – Source of destabilization in politics, economics, the ICT space	– Conducts revisionist policy – Expands the scope of malicious activity in the ICT space – Uses ICT to achieve aggressive foreign policy goals – Violates human rights using ICT

Note. The connotative coloring of securitization objects within the discourse under consideration is the main criterion for classifying threats.

Source: compiled by L.M. Sokolshchik, I.O. Yanikeeva, and G.V. Toropchin, based on the content analysis of an American official documents database.

Content Analysis of Threats Attributed to State Actors

In the quantitative content analysis, each document in the collected dataset was examined for references to ICT security threats. The results of the analysis provide an insight into the specific state actors mentioned in direct connection with the specific ICT security threats emanating from them. The associated ICT security threats for each state are visually presented in both Table 2 and in Figures 1–4 (using a cloud of "tags" (keywords), where the font size depends on the number of specific threats' mentions).

The results of the quantitative content analysis of the corpus of documents on ICT security in the context of U.S. relations with Latin American countries can be interpreted as follows.

Table 2. **ICT Security Threats Attributed to State Actors by Number of Mentions**

Threat	Russia	China	Iran	DPRK
Aggressive intelligence operations	1	1	1	–
Ransomware	2	1	1	2
Malware	–	–	1	–
Disinformation	2	1	–	–
Destabilizing cyberactivities	2	–	–	–
Cyberattacks	3	2	1	2
Cyberinfluence	3	–	–	–
Cyberoperations	1	1	2	–
Cybercrime	–	–	–	2
Cyberdisruptions	1	–	–	–
Cyberthreat	4	4	1	–
Cyberespionage	3	2	–	2
Information manipulation	1	–	–	–
Influence operations	–	1	–	–
Efforts to erase data	1	–	–	–
Appropriation of cyberinfrastructure	–	–	–	1
Seized cryptocurrency	–	–	–	1
Threat to technological competitiveness	–	4	–	–
Digital authoritarianism	–	2	–	–

Source: compiled by L.M. Sokolshchik, I.O. Yanikeeva, and G.V. Toropchin, based on the content analysis of an American official documents database.

Figure 1. Threats to ICT Security Attributed to the Russian Federation:
the font size is a function of the number of mentions
Source: compiled by G.V. Toropchin based on Table 2.

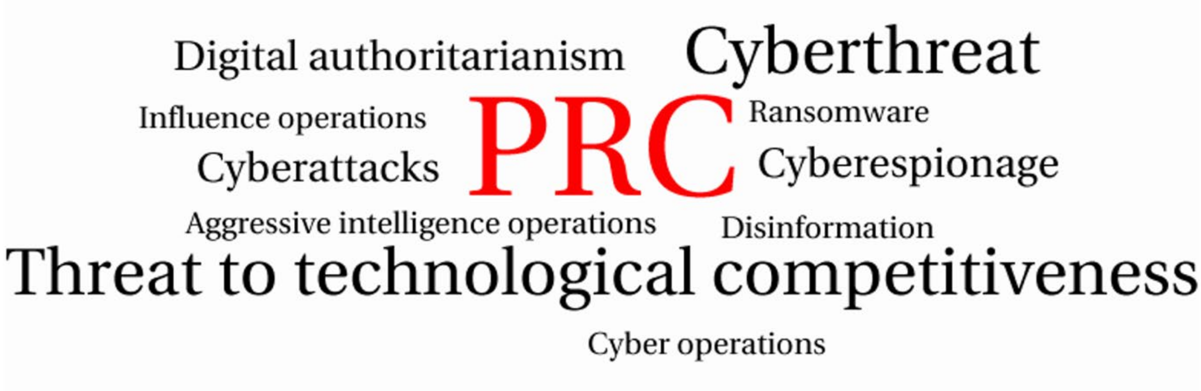

Figure 2. Threats to ICT Security Attributed to the PRC:
the font size is a function of the number of mentions
Source: compiled by G.V. Toropchin based on Table 2.

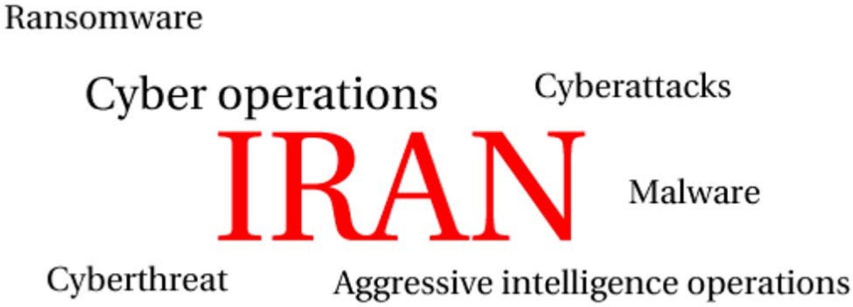

Figure 3. Threats to ICT Security Attributed to Iran:
the font size is a function of the number of mentions
Source: compiled by G.V. Toropchin based on Table 2.

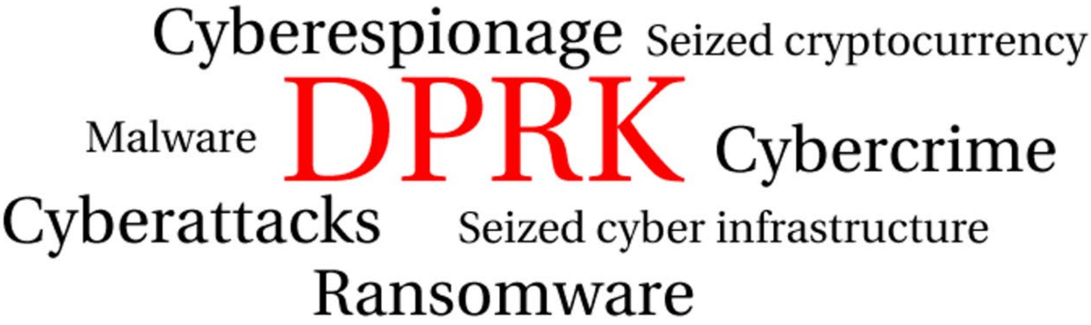

Figure 4. Threats to ICT security attributed to the DPRK:
the font size is a function of the number of mentions
Source: compiled by G.V. Toropchin based on Table 2.

It is precisely four powers — Russia, China, Iran, and the DPRK — that are presented to the recipient, i.e. Latin American countries, as the main sources of threats in the ICT space. The range of specific associations regarding ICT security threats turns out to be quite diverse. All four state actors are attributed with cyberattacks and ransomware, three states except for the DPRK — with aggressive intelligence operations, cyber operations, and threats to digital infrastructure in general. Finally, three countries, excluding Iran, are attributed with cyber espionage activities.

Of particular note is the fact that the Biden administration considered China's striving for superiority in the ICT sphere to be the most pressing security concern. The second most significant threat is emanating from Russia due to its intention to strengthen its ICT capabilities and to undermine U.S. influence. Accordingly, the activities of Chinese and Russian companies in the IT markets of the Latin American region providing ICT security services are interpreted as undesirable. At the same time, the ICT threats attributed to Russia in the documents are repeatedly linked to its special military operation in Ukraine, thereby confirming the conclusion regarding the use of ideological arguments in the promotion of American ICTs in Latin America.

Conclusion

A critical analysis of the Biden administration's discourse on ICT security has revealed the mechanisms by which the hidden ideology of U.S. dominance in Latin America is implemented. The research found that official discourse plays a central role in legitimizing U.S. hegemonic aspirations, presenting them as aimed at protecting democratic values and ensuring global stability. The cognitive model of the contextual "field" presented in the American discourse reflects the desire of the United States to maintain its leadership in the global ICT space. This is achieved by strengthening its position through multilateral institutions and regional cooperation, while simultaneously counteracting the influence of other major powers, primarily China and Russia, by constructing the image of Washington as the exclusive provider of international ICT security.

By constructing the "agent — recipient — object" figurative system through discursive referential and predicational strategies, as well as an argumentation system, the United States seeks to justify its active role in Latin America, to consolidate the passive position of Latin American countries, and to legitimize the discriminated position of China, Russia, Iran, and the DPRK both in the ICT sphere in general and as actors in Latin America. At the same time, this discursive construct substantiates the possibility, and even the necessity, of U.S. intervention in regional and domestic political processes in the ICT security field. While the American discourse seeks to justify this figurative system with technological, economic, value-based, and altruistic arguments, it ultimately turns out to be politically motivated, with the rhetoric of cooperation largely serving to advance American strategic interests in the region.

A key direction for future research is analyzing how Latin American countries perceive U.S. discourse on ICT security. Understanding how regional actors interpret and respond to this could help to better understand the process of international interaction in this sphere. Furthermore, the research of alternative models of the international ICT space and its security is promising. An in-depth study of the role of other major actors, such as the EU, China, and Russia, in shaping ICT security policy in the Latin American region is also needed to provide a broader context for the analysis.

Received / Поступила в редакцию: 17.01.2025
Revised / Доработана после рецензирования: 07.04.2025
Accepted / Принята к публикации: 10.06.2025

References

Bolgov, R. (2020). The UN and cybersecurity policy of Latin American countries. *2020 7th International Conference on eDemocracy and eGovernment*, ICEDEG 2020 (pp. 259–263). Buenos Aires: Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICEDEG48599.2020.9096798; EDN: CFHGPI

Buzan, B., Weaver, O., & de Wilde, J. (1998). *Security: A new framework for Analysis*. London: Boulder, Lynne Rienner Publishers. Retrieved from https://www.academia.edu/39047709/Buzan_Waever_and_De_Wilde_1998_Security_A_New_Framework_For_Analysis

Campbell, D. (1993). *Politics without principle: Sovereignty, ethics, and the narratives of the Gulf War*. Boulder, USA: Lynne Rienner Publishers. https://doi.org/10.1515/9781685856090

Fomin, I. V. (2014a). Representations of state formations in political discourse analysis (the case of Kosovo). *Polis. Political Studies*, (2), 124–137. (In Russian). https://doi.org/10.17976/jpps/2014.02.09; EDN: RXHOPN

Fomin, I. V. (2014b). The category of image as a means of studying the political reality (the example of the image of South Ossetia in the Russian foreign policy discourse). In *Symbolic politics: Collection of articles* (Issue 2: Debates on the Past as Designing the Future, pp. 40–65). Moscow: Institut nauchnoi informatsii po obshchestvennym naukam RAN publ. (In Russian). EDN: ULCLXR

Henshaw, A. (2024). Capacity building and cyber insecurity in Latin America: Geopolitics, Surveillance, and Disinformation. In A. Mhajne & A. Henshaw (Eds.), *Critical perspectives on cybersecurity: Feminist and postcolonial interventions* (pp. 173–193). New York: Oxford University Press. https://doi.org/10.1093/oso/9780197695883.003.0008

Hurel, L. M. (2022). Interrogating the cybersecurity development agenda: A critical reflection. *The International Spectator*, 57(3), 66–84. https://doi.org/10.1080/03932729.2022.2095824; EDN: SPVBPZ

Kheifets, V. L., & Khadorich, L. V. (2015). Latin America between OAS and CELAC. *World Economy and International Relations*, (4), 90–100. (In Russian). https://doi.org/10.20542/0131-2227-2015-4-90-100; EDN: TRNTVZ1`

Krebs, R. R. (2015). How dominant narratives rise and fall: Military conflict, politics, and the Cold War consensus. *International Organization*, 69(4), 809–845. https://doi.org/10.1017/S0020818315000181

Krutskikh, A. V. (2022). International information security: In search of consolidated approaches : Interview with Andrey V. Krutskikh, Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security. Interviewed by D. A. Piskunov. *Vestnik RUDN. International Relations*, 22(2), 342–351. https://doi.org/10.22363/2313-0660-2022-22-2-342-351; EDN: DVBISA

Miao, W., Xu, J., & Zhu, H. (2019). From technological issue to military-diplomatic affairs: Analysis of China's official cybersecurity discourse (1994–2016). In J. Hunsinger, M. Allen & L. Klastrup (Eds.), *Second international handbook of internet research* (pp. 1–13). Dordrecht: Springer. https://doi.org/10.1007/978-94-024-1202-4_61-1

Pakhalyuk, K. A. (2018). Intellectual origins of discursive analysis in political studies. *Moscow State University Bulletin. Series 18. Sociology and Political Science*, 24(1), 71–97. (In Russian). https://doi.org/10.24290/1029-3736-2018-24-1-71-97; EDN: YUPBIH

Ponka, T. I., Ramich, M. S. & Wu, Y. (2020). Information policy and information security of PRC: Development, approaches and implementation. *Vestnik RUDN. International Relations*, 20(2), 382—394. https://doi.org/10.22363/2313-0660-2020-20-2-382-394; EDN: UANODL

Reisigl, M., & Wodak, R. (2009). The discourse-historical approach (DHA). In R. Wodak & M. Meyer (Eds.), *Methods of critical discourse analysis:* 2nd revised edition (pp. 87–121). London: SAGE. Retrieved from https://www.researchgate.net/publication/251636976_The_Discourse-Historical_Approach_DHA

Siudak, R. (2022). Cybersecurity discourses and their policy implications. *Journal of Cyber Policy*, 7(3), 318–335. https://doi.org/10.1080/23738871.2023.2167607; EDN: MLSWMA

Sokolshchik, L. M., Sakaev, V. T., & Galimullin, E. Z. (2023). Illegal immigration from Latin America amid the 2024 U.S. presidential campaign: Polarization effects. *Journal of International Analytics*, 14(3), 106–126. (In Russian). https://doi.org/10.46272/2587-8476-2023-14-3-106-126; EDN: FTAYME

Sokolshchik, L. M., Sokolshchik, Yu. S., & Teremetskiy, K. S. (2024). Discursive strategies for legitimizing U.S. sanctions policy towards Russia (2021–2023). *Polis. Political Studies*, (3), 109–125. (In Russian). https://doi.org/10.17976/jpps/2024.03.08; EDN: NTYWXM

Sokolshchik, L. M. (2024). Year one of the Biden administration: U.S. foreign policy Towards Russia. *Journal of Eurasian Studies*, 15(1), 70–80. https://doi.org/10.1177/18793665231170639; EDN: AMHXNS

Sokolshchik, L., & Sokolshchik, Y. (2023). Why U.S. – Russia relations failed: an analysis of competing national security narratives. *Russian Politics*, 8(4), 468–492. https://doi.org/10.30965/24518921-00803009; EDN: YFYVMB

Stadnik, I. T. (2024). How to study ICT-security policy: Opportunities and challenges for critical discourse-analysis. *Vestnik of Saint Petersburg University. International Relations*, 17(2), 183–200. (In Russian). https://doi.org/10.21638/spbu06.2024.205; EDN: NKMILI

Svirchevskii, D. A., & Fomin, I. V. (2023). Images of Europe in the discourse of German left- and right-wing populists: Between solidarity Europe and fortress Europe. *Polis. Political Studies*, (2), 27–40. (In Russian). https://doi.org/10.17976/jpps/2023.02.03; EDN: YGNOEA

Tikk, E., & Kerttunen, M. (2020). Introduction. In E. Tikk & M. Kerttunen (Eds.), *Routledge handbook of international cybersecurity* (pp. 1–8). New York: Routledge. https://doi.org/10.4324/9781351038904

Urbanovics, A. (2022). Cybersecurity policy-related developments in Latin America. *AARMS — Academic and Applied Research in Military and Public Management Science*, 21(1), 79–94. https://doi.org/10.32565/aarms.2022.1.6; EDN: JOBKFG

Van Dijk, T. A. (2006). Discourse, context and cognition. *Discourse Studies*, 8(1), 159–177. https://doi.org/10.1177/1461445606059565

Wendt, A. (1999). *Social theory of international politics*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511612183

Zinovieva, E., & Ignatov, A. (2023). The role of BRICS in the international ICT security regime. *International Trends / Mezhdunarodnye Protsessy*, 21(4), 104–132. (In Russian). https://doi.org/10.17994/IT.2023.21.4.75.2; EDN: AVLWZW

About the authors:

Sokolshchik Lev Markovich — PhD (History), Leading Researcher, Center for Comprehensive European and International Studies, National Research University Higher School of Economics; 17 Malaya Ordynka St, Moscow, 119017, Russian Federation; eLibrary SPIN-code: 6958-8932; ORCID: 0000-0002-0945-1022; e-mail: lsokolshchik@hse.ru

Yanikeeva Inna Olegovna — PhD (Political Science), Researcher, Center for Comprehensive European and International Studies, National Research University Higher School of Economics, 17 Malaya Ordynka St, Moscow, 119017, Russian Federation; eLibrary SPIN-code: 5148-7454; ORCID: 0000-0001-9590-5301; e-mail: iyanikeeva@hse.ru

Toropchin Gleb Vyacheslavovich — PhD (History), Associate Dean for Academic Affairs, Faculty of Humanities, Novosibirsk State Technical University; 20 K. Marksa Avenue, Novosibirsk, 630073, Russian Federation; Senior Research Fellow, Center for Eurasian Studies, National Research Tomsk State University; 36 Lenina Avenue, Tomsk, 634050, Russian Federation; eLibrary SPIN- code: 1524-2434; ORCID: 0000-0002-8055-1202; e-mail: glebtoropchin@mail.ru