Vestnik RUDN. International Relations. ISSN 2313-0660 (Print), ISSN 2313-0679 (Online)
Вестник РУДН. Серия: МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ
2025 Vol. 25 No. 3 469–484
http://journals.rudn.ru/international-relations

# ПРИКЛАДНОЙ АНАЛИЗ

# APPLIED ANALYSIS

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

*Научная статья / Research article*

## 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

# 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

## Введение

Проблема безопасности в области информационно-коммуникационных технологий (ИКТ) в последние десятилетия стала неотъемлемой частью политической повестки на международном и национальном уровнях. Усиливается интерес к данной теме и со стороны научного сообщества (Крутских, 2022; Понька, Рамич, У, 2020; Bolgov, 2020; Henshaw, 2024; Hurel, 2022). При этом на уровне Организации Объединенных Наций (ООН) признается, что ИКТ-проблематика все больше политизируется[1]. Нередко за стремлением обеспечить безопасность в этой сфере скрываются гегемонистские устремления международных игроков. Одним из характерных примеров реализации подобной логики может служить внешняя политика США в отношении Латинской Америки при администрации Дж. Байдена.

В научной литературе пока не сформировалось единого понятийного аппарата, описывающего данную область изучения. Существует ряд подходов к пониманию безопасности в ИКТ-сфере. Широкая трактовка охватывает информационную безопасность и включает все аспекты безопасности в цифровой среде, в том числе политические. Узкая трактовка подразумевает под кибербезопасностью технические вопросы предотвращения угроз и рисков для цифровой инфраструктуры, программного обеспечения и оборудования (Зиновьева, Игнатов, 2023, с. 107–108).

Нередко в исследованиях понятия «кибербезопасность» и «информационная безопасность» смешиваются и используются как синонимы. В связи с этим в работе применяется аналитическая категория «ИКТ-безопасность» как компромиссный термин, включающий весь спектр вопросов безопасности в рассматриваемой области (Зиновьева, Игнатов, 2023, с. 107–108) и предполагающий противодействие угрозам в ИКТ-сфере, а также угрозам, возникающим при использовании ИКТ, в военно-политическом, политико-идеологическом, общественном, экономическом, инфраструктурном и технологическом измерениях.

Несмотря на то, что Вашингтон официально придерживается трактовки безопасности в ИКТ-сфере, соотносящейся с понятием «кибербезопасность», в американском дискурсе присутствуют элементы более широкого концепта информационной безопасности, включающего борьбу с кибертерроризмом, дезинформацией и информационным вмешательством во внутренние дела государства[2]. В этом плане использование широкого понятия «ИКТ-безопасность» применительно к американскому кейсу представляется более чем оправданным.

США играют важную роль в цифровой трансформации мира. Они стояли у истоков Интернета и в настоящее время активно используют свой потенциал в сфере ИКТ для реализации целей внешней политики. Одним из способов выстраивания властных отношений являются дискурсивные практики как систематические и спланированные речевые акты политических агентов (Сокольщик, Сокольщик, Теремецкий, 2024, с. 113). Во многом из-за своего прикладного значения для внешней политики вопросы ИКТ-безопасности достаточно редко рассматриваются в дискурсивном измерении. Данное исследование призвано заполнить эту лакуну за счет комплексного исследования дискурса о безопасности в ИКТ-пространстве в период администрации Дж. Байдена в рам-

[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).

ках латиноамериканского направления внешней политики США.

Дискурсы США, содержащиеся в официальных материалах по тематике ИКТ-безопасности, отражают международные амбиции Вашингтона в условиях трансформирующегося международного порядка. С момента провозглашения «доктрины Монро» в первой четверти XIX в. Латинская Америка входит в число наиболее приоритетных регионов для реализации внешней политики США. Закономерно, что регион занимает одно из центральных мест в рассматриваемом дискурсе. При этом с точки зрения США Латинская Америка очень уязвима в ИКТ-пространстве, поэтому она нуждается в патернализме со стороны Вашингтона.

Под Латинской Америкой в работе понимается весь континент Южной Америки, а также Мексика, страны Центральной Америки и острова Карибского бассейна, жители которых говорят на романских языках (Сокольщик, Сакаев, Галимуллин, 2023, с. 108).

Фундаментальной предпосылкой для исследования выступает конструктивистская идея о том, что политическая реальность существует не сама по себе, ее значение для нас является продуктом социального конструирования и интерпретаций со стороны различных агентов (Campbell, 1993), которые преследуют политические цели (Krebs, 2015, p. 810). Агенты создают субъективный мир политики, который не тождественен объективной реальности, хотя может иметь в ней референты (Сокольщик, Сокольщик, Теремецкий, 2024, с. 111; Sokolshchik, 2024). Государства как основные агенты на мировой арене в процессе коммуникативной интеракции взаимно признают право на суверенитет, легитимизируя существование друг друга и формируя саму систему международных отношений (Wendt, 1999, pp. 10–11). Конструирование политического бытия агентами происходит за счет создания дискурсов, которые не только отражают политические отношения, но и оказывают на них серьезное влияние (Miao, Xu & Zhu, 2019, p. 2).

В контексте исследования важное значение имеет процесс секьюритизации (Buzan, Wæver & de Wilde, 1998) как дискурсивная практика (Sokolshchik & Sokolshchik, 2023), при которой *агент* обозначает некий *объект* в качестве угрозы безопасности и приводит *реципиенту* аргументы в пользу контрмер в отношении этого секьюритизированного объекта (Miao, Xu & Zhu, 2019, p. 2).

Цель исследования заключается в анализе идеологии, которая скрывается в дискурсе США по проблематике ИКТ-безопасности на латиноамериканском направлении, поддерживая и оправдывая властные отношения между Вашингтоном и государствами региона.

Дискурс об ИКТ-безопасности анализируется на глобальном и национальном уровнях как комплекс опасений и угроз (Tikk & Kerttunen, 2020). Применительно к страновым случаям метод контент-анализа используется к доктринальным документам в области ИКТ-безопасности ряда латиноамериканских стран (Аргентина, Бразилия, Колумбия, Мексика, Перу, Чили) (Urbanovics, 2022). Р. Сюдак выделяет два основных типа дискурса ИКТ-безопасности с точки зрения их влияния на политику: технический дискурс и дискурс национальной безопасности (Siudak, 2022).

Потенциал критического дискурс-анализа (КДА) был опробован в ходе анализа двусторонних отношений США и России в области ИКТ-безопасности в работе И.Т. Стадник (2024). В целом работы, исследующие дискурсивное конструирование ИКТ-безопасности и критически осмысляющие его структуры, носят фрагментарный характер.

## Методологическая и источниковая база исследования

Методологическую рамку исследования формирует КДА в сочетании с методом количественного контент-анализа. КДА подразумевает выявление в речи *агента* скрытой идеологии, которая поддерживает социальную власть, доминирование и неравенство. Отправной точкой для КДА служит предположение о том, что посредством дискурса *агент* навязывает *реципиенту* тот или иной

образный или символический порядок в качестве исключительно правильного (Пахалюк, 2018, с. 165). В подобном ракурсе под дискурсом понимается политический акт и способ воспроизводства власти.

Исследование фокусируется на прагматическом аспекте дискурса (Фомин, 2014a, с. 129), поскольку он соотносится с некоторой частью социополитической реальности или «полем действия» (Reisigl & Wodak, 2009, pp. 90–91). Это «поле» конструируется агентом через *когнитивные модели*, которые задают контекст для дискурса (van Dijk, 2006, p. 163), отражая связи между личными знаниями о событиях, с одной стороны, и разделяемыми обществом убеждениями — с другой. Как отмечает Т. ван Дейк, когнитивные модели контекста являются основой «прагматического» понимания дискурса в силу того, что их структура обусловливает его реализацию и понимание (van Dijk, 2006, pp. 168–170).

С учетом специфики предмета исследования в работе «поле действия» определяется как конструируемая США когнитивная модель международного ИКТ-пространства, которая выступает в качестве контекста для частного случая дискурса об ИКТ-безопасности на латиноамериканском направлении. В рамках когнитивной модели международного ИКТ-пространства США выделяются следующие структурные элементы: *глобальное* и *региональное измерения*, а также *ИКТ-угрозы* и *методы / инструменты их решения*.

В сфере коммуникативного взаимодействия скрытая идеология реализуется через конструируемые *образы агента*, *реципиента* и *объектов* секьюритизации (Фомин, 2014b, с. 51). В данном случае образ осмысляется как «семиотическая конструкция, формируемая в рамках того или иного дискурса и аккумулирующая акты осмысления и означивания, характерные для этого дискурса» (Свирчевский, Фомин, 2023, с. 29). Образы создаются через дискурсивные стратегии, которые можно определить как намеренно реализуемые планы агента по использованию языка для достижения политических целей (Фомин, 2014a, с. 129). Выделяют следующие основные дискурсивные стратегии: *референция* (конструирование явлений, акторов, процессов), *предикация* (атрибутирование позитивных или негативных характеристик явлений, акторов, процессов) и *аргументация* (обоснование / оспаривание истинности тезисов).

Таким образом, в данном исследовании КДА был проведен на 1) контекстуальном уровне («поле действия») — через анализ *когнитивной модели международного ИКТ-пространства США* как контекста рассматриваемого дискурса и 2) дискурсивном уровне — через анализ *образов агента* (США), *реципиента* (Латинская Америка) и *объектов секьюритизации*, создаваемых посредством дискурсивных стратегий *референции* и *предикации,* а также приводимой в пользу конструируемой образной системы *аргументации.*

Дополняет качественный анализ количественный контент-анализ, который применяется для исследования частотности упоминаний в корпусе источников *объектов* в качестве угроз и предлагаемых политических решений. Для проведения контент-анализа использовалось программное обеспечение *QDA Miner Lite*[3], посредством которого был проведен анализ собранного корпуса документов внешней политики США, загруженного в приложение для определения частоты упоминаний государственных акторов как объектов секьюритизации и атрибутируемых ими угроз.

Источниковая база исследования состоит из материалов официальных сайтов государственных органов США (Белый дом, Государственный департамент, Министерство обороны, Министерство юстиции, Министерство внутренней безопасности). Хронологические рамки исследования охватывают период с 20 января 2021 г. (инаугурация президента Дж. Байдена) до 13 ноября 2024 г. (последние доступные данные на момент написания текста исследования).

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

Сбор данных был осуществлен в три этапа. Первоначально был произведен поиск по лексическому маркеру «Латинская Америка» (*Latin America*). Затем из полученного массива были извлечены документы, содержащие лексемы «кибер-» (*cyber*), «цифровой» (*digital*), «искусственный интеллект» (*artificial intelligence*). На завершающей стадии была осуществлена выборка документов, непосредственно относящихся к теме ИКТ-безопасности, через поиск лексического маркера «безопасность» (*security*). Таким образом, для анализа было отобрано 47 документов[4]. Основной массив данных был дополнен материалами СМИ, международных организаций, международных проектов в области ИКТ-безопасности, а также аналитических центров.

## Когнитивная модель международного ИКТ-пространства

### *Глобальное измерение*

В рамках американского дискурса констатируется факт, что международная система переживает кризис. Эпоха мирового развития, начавшаяся после распада биполярной системы, завершается. В международных отношениях на первый план выходит великодержавное соперничество за влияние в ключевых регионах, среди которых значится Латинская Америка, и различных областях, включая ИКТ. В этой связи в американских официальных документах и заявлениях акцентируется необходимость сохранения доминирования страны на мировой арене. Постулируется, что центральную роль в продвижении интересов США играет лидерство в ИКТ-пространстве, цифровой экономике и новых технологиях. Утверждается также, что первенство США в сфере ИКТ не только укрепляет национальную безопасность страны, но и поддерживает демократические ценности и способствует «улучшению жизни людей во всем мире»[5].

В рамках американской концепции ИКТ-пространства особое внимание уделяется институциональному аспекту, международным нормам и сотрудничеству. Заявляется, что США совместно с партнерами стремятся укрепить многосторонние институты, в частности ООН, для совершенствования правил взаимодействия в этой области. При этом подчеркивается, что международные нормы должны быть «справедливыми» по отношению к американским рабочим и корпорациям, защищая «конкуренцию» и поддерживая экономическое и технологическое превосходство США[6]. Таким образом, глобальный институциональный каркас ИКТ-пространства — в представлениях Вашингтона — должен поддерживать доминирующее положение США в мировой экономике и политике.

Вместе с тем заявляется, что противники США стремятся использовать международные институты для достижения целей, которые противоречат американским интересам[7].

[4] Среди них см., например: 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. 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).

США описывают Россию и Китай как страны, которые используют многосторонние институты, в том числе ООН, для оказания влияния на развивающиеся страны и предпринимают попытки изменить нормы в ИКТ-пространстве. При этом разделение мира осуществляется на основе идеологической антитезы «демократия — автократия». Подобный дискурс призван сформировать образ мира, в котором цифровизация приносит пользу государствам только в том случае, если процесс возглавляет Вашингтон.

Поскольку продвижение интересов США в рамках Совета Безопасности ООН ограничено правом вето Китая и России, Вашингтон попытался подменить универсальные институты «саммитами за демократию»[8]. Через подобные форумы США стремились выдать свою ИКТ-повестку за мнение «международного сообщества». В частности, на саммитах в 2023 и 2024 гг., помимо прочего, было подчеркнуто обязательство стран-участниц развивать «новые технологии в соответствии с демократическими ценностями и правами человека»[9]. При этом основным критерием для «демократичности» той или иной страны служат партнерские отношения с США. Таким образом, происходит оправдание дискриминационного дискурса США с помощью разграничения по принципу «свой — чужой» (Сокольщик, Сакаев, Галимуллин, 2023, с. 119).

### *Региональное измерение*

Для успешной реализации ИКТ-повестки на региональном уровне администрация Дж. Байдена стремилась использовать такие многосторонние форумы, как Организация американских государств (ОАГ). Учрежденная на заре холодной войны под эгидой США, ОАГ объединила все государства Северной и Южной Америки, кроме Кубы, и стала стержнем межамериканский системы международных отношений (Хейфец, Хадорич, 2015, с. 94). Организация во многом осталась проводником интересов США и после завершения биполярного противостояния (Хейфец, Хадорич, 2015, с. 94–96). В рассматриваемом дискурсе подчеркивается, что США оказывают содействие усилиям ОАГ в таких областях, как реагирование на инциденты в ИКТ-пространстве, повышение осведомленности об ИКТ-безопасности и подготовке кадров для работы в этой сфере. При этом ОАГ с 2003 г. реализует «Программу кибербезопасности», которая призвана формировать концептуальные основы для национальных стратегий стран-участниц в этой области[10].

Кроме того, ОАГ является коллективным членом международных платформ в области ИКТ-безопасности, осуществляющих свою деятельность под эгидой США, в частности Международной инициативы по борьбе с программами-вымогателями[11] и Глобального форума по киберэкспертизе[12]. Ряд стран Латинской Америки самостоятельно участвуют в инициативах и партнерствах в области ИКТ-безопасности при лидирующей роли США, среди которых можно отметить Декларацию о будущем Интернета (Аргентина, Колумбия, Коста-Рика, Перу, Тринидад и Тобаго, Уругвай)[13] и Коалицию за свободу в Интернете (Аргентина, Колумбия, Коста-Рика, Мексика, Чили)[14]. Опора на ОАГ и другие многосторонние институты позволяет

[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).

[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).

повысить координацию при продвижении американской повестки на региональном уровне и представить действия США как проводника «коллективной» ИКТ-безопасности. Кроме того, США активно развивают сотрудничество на двусторонней основе, взаимодействуя почти со всеми странами региона.

### *Угрозы в ИКТ-пространстве*

В американском дискурсе можно выделить четыре обширные области, где проявляются ИКТ-угрозы, которые в целом соотносятся с классификацией Министерства внутренней безопасности США[15]:

1) общественная безопасность (например, распространение дезинформации, кибертерроризм, вмешательство в выборы);

2) охрана границ и миграционная безопасность (например, транснациональные криминальные организации);

3) безопасность критической инфраструктуры (например, кибератаки и кибершпионаж в отношении объектов энергетики и транспорта);

4) экономическая безопасность (например, кибератаки и кибершпионаж в финансовых целях, манипулирование рынками).

Руководство США заявляет, что международные конфликты все чаще разворачиваются в ИКТ-пространстве, усиливая риски для безопасности США и их союзников[16]. Среди государственных акторов, которые воспринимаются США в качестве ключевых угроз в ИКТ-сфере, в первую очередь выделяются Китай и Россия. Список дополняют Корейская Народно-Демократическая Республика (КНДР) и Исламская Республика Иран (ИРИ).

Американский дискурс также содержит описание следующих методов / инструментов противодействия ИКТ-угрозам:

– укрепление союзов и партнерств в ИКТ-сфере (коллективная кибероборона);

– расширение деятельности на базе международных организаций и институтов;

– разработка международных норм и правил в ИКТ-пространстве, в том числе в области искусственного интеллекта (ИИ);

– создание международных правоохранительных механизмов в ИКТ-пространстве;

– идеологизация повести ИКТ-безопасности через разделение мира по принципу «свой — чужой»;

– расширение присутствия США, в том числе агентов спецслужб, за рубежом;

– усиление контроля над экспортом и распространением передовых ИКТ и компонентов;

– инвестиции в национальную ИТ-отрасль, в том числе ИИ, 5G и 6G, облачную инфраструктуру, центры обработки данных;

– оказание международной помощи развитию в ИКТ-сфере, включая подготовку специалистов;

– применение санкций для обеспечения национальных интересов и безопасности в ИКТ-пространстве.

## Скрытая идеология в дискурсе США

### *Образ агента*

США как агент дискурсивного процесса стремятся продвинуть на международной арене свое представление об ИКТ-безопасности как исключительное и истинное. Вашингтон преподносит себя как «защитника свободы и демократии», «лидера в технологиях», «партнера по безопасности», подчеркивая свою уникальную роль в противодействии ИКТ-угрозам и заинтересованность в сотрудничестве. Постулируется, что США должны играть ведущую роль в формировании глобальных норм и институтов ИКТ-пространства, особенно применительно к сфере ИИ. В рамках американского дискурса утверждается, что США на протяжении всей своей истории были мировым лидером в развитии передовых технологий, которые они использовали не только для укрепления своей

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

национальной безопасности, но и для продвижения демократии во всем мире[17].

США склонны гиперболизировать свои положительные качества и маскировать стремление к доминированию в Латинской Америке. Деятельность США в области ИКТ-безопасности описывается как исключительное благо для региона, поскольку они стремятся укрепить потенциал латиноамериканских стран в ИКТ-сфере для защиты прав человека и демократии, их экономического и технологического развития, укрепления суверенитета. В подобной интерпретации успешное развитие стран Латинской Америки возможно только при использовании технологических решений США, поскольку только они могут предоставить «безопасную цифровую инфраструктуру». Тем самым США формируют свой образ как незаменимого «поставщика» ИКТ-безопасности для латиноамериканских стран.

### *Образ реципиента*

Как уже отмечалось, в представлении США Латинская Америка — регион с высоким уровнем уязвимости в ИКТ-пространстве, который нуждается в патернализме. Это, с одной стороны, позволяет оправдывать приниженное и преимущественно пассивное положение латиноамериканских государств, а с другой — лидирующую и априори активную роль США в регионе. Учитывая значимость многостороннего подхода, в который нередко облекается американский гегемонистский дискурс, США отмечают, что страны Латинской Америки «вносят свой вклад в коллективные усилия по развитию киберпространства»[18].

Руководство США характеризует Западное полушарие как сообщество единомышленников для убеждения реципиента в необходимости совместных действий в ИКТ-пространстве так, как это видят США. За американскими тезисами скрывается намерение убедить Латинскую Америку в важности выбора в качестве партнера в цифровой среде Вашингтона, а не кого-то «чужого». Дискурс усиливается заявлениями о том, что для США в приоритете, чтобы в регионе присутствовали «надежные поставщики» ИКТ-безопасности, коим может выступать только Вашингтон.

С точки зрения США, латиноамериканские страны не способны на самостоятельное развитие в ИКТ-пространстве. Модель неравных отношений имплицитно содержится практически во всех аспектах рассматриваемого дискурса, в том числе в вопросе помощи развитию. Американский дискурс акцентирует низкий технологический уровень стран региона и широкие возможности США для помощи их развитию в данной области. Отмечается, что латиноамериканским странам приходится, в частности, делать «выбор между инвестициями в цифровое будущее или в возобновляемые источники энергии»[19], в то время как США готовы вкладывать ресурсы в регион для поддержки его цифрового развития, например инфраструктуры 5G.

### *Образы объектов секьюритизации*

Среди государственных акторов в американском дискурсе в области ИКТ-безопасности в качестве основных угроз и источников дестабилизации для Латиноамериканского региона обозначаются Китай и Россия. Пекин описывается как «стратегический конкурент, способный угрожать

[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).

[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).

интересам США и доминировать в области новых технологий». Москва представляется в качестве «постоянной киберугрозы, поскольку совершенствует свои возможности» для ослабления альянсов и партнерств США[20]. Вместе с тем заявляется, что страны Латинской Америки обеспокоены возможностью дезинформации со стороны России: «США оказали техническую помощь и поддержку, чтобы колумбийские институты смогли защитить свою инфраструктуру и противостоять [российской] дезинформации»[21]. При этом деятельность Китая позиционируется как более серьезная угроза для США и всех стран Латинской Америки, так как Пекин стремится превзойти Вашингтон в сфере ИКТ и предлагает комплексные решения развития в этой области. Образ Китая формируется как системная угроза США по всему спектру вопросов ИКТ-безопасности. Так, в американском дискурсе постулируется, что «за последние 10 лет Китай расширил сферу кибероперацийи… став самым продвинутым стратегическим конкурентом США, способным угрожать американским интересам и доминировать в области новых технологий»[22]. В свою очередь Россия, по мнению США, постепенно наращивает ИКТ-потенциал для расширения «вредоносной» деятельности против США, в том числе в Латинской Америке. Утверждается, что Россия стремится сохранить влияние в Западном полушарии за счет развития сотрудничества с узким кругом стран, состоящим из Аргентины, Бразилии, Венесуэлы, Кубы и Никарагуа[23].

На втором плане американского дискурса присутствуют КНДР и Иран, которые представляют ограниченную угрозу, но увеличивают масштабы «вредоносной деятельности» в ИКТ-пространстве[24]. Иран «использует киберпотенциал для угроз союзникам США», а КНДР «получает доходы от преступной деятельности» с использованием ИКТ[25]. Констатируется, что дальнейшее развитие возможностей этих стран в ИКТ-сфере может оказать серьезное влияние на безопасность США и их партнеров[26].

Таким образом, державы, способные предложить альтернативный американскому путь развития стран Латинской Америки в рассматриваемой сфере, то есть в первую очередь Китай и Россия, однозначно маркируются в дискурсе США в качестве наиболее значимых ИКТ-угроз.

### *Аргументация*

Для легитимации образной системы «агент — реципиент — объект» (табл. 1) США используют широкий спектр аргументов. Они стремятся обосновать свою особую роль для Латинской Америки через тезис об общей безопасности и акцентируют внимание на необходимости коллективных действий. Это позволяет им выступать в роли координатора многосторонних усилий в области ИКТ-безопасности. Утверждается, что партнерство с латиноамериканскими странами имеет решающее значение для формирования общего видения киберпространства. Приводятся аргументы о тесных экономических связях и общих ценностях стран Северной

[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).

[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.

и Южной Америки. Активно используется идеологически окрашенная аргументация. Так, постулируется, что «страны, ответственно использующие цифровые технологии, соблюдающие права человека и демократические ценности, становятся сильнее, когда работают вместе»[27]. При этом имплицитно подразумевается, что совместная деятельность должна осуществляться при лидирующей роли США.

Вашингтон использует гипотетические сценарии, например, возможный коллапс критической инфраструктуры и масштабные кибератаки для обоснования необходимости своего присутствия в регионе. Вместе с тем в американском дискурсе прослеживается риторика альтруизма. Политика США преподносится как направленная исключительно на защиту прав человека и демократических институтов. Действительно, США оказывают широкую техническую и экспертную помощь странам Латинской Америки в разработке стратегий ИКТ-безопасности, создании центров реагирования на инциденты, укреплении инфраструктуры и борьбе с международной преступностью, использующей ИКТ[28]. Нередко политика помощи преподносится как проявление «доброй воли» США. При этом скрытые стратегические цели, такие как усиление экономического и политического влияния в регионе, остаются неявными.

[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] См.: 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).

## Контент-анализ атрибутируемых государственным акторам угроз

В ходе проведения количественного контент-анализа каждый документ из собранного массива данных был изучен на предмет упоминания угроз в ИКТ-пространстве. Результаты анализа представленной выборки дают представление о конкретных государственных акторах, упоминаемых в непосредственной связке с исходящими от них конкретными угрозами в сфере ИКТ-безопасности. Связанные угрозы в области ИКТ-безопасности для каждого государства визуально представлены в табл. 2 и при помощи облака «тэгов» (ключевых слов), где размер шрифта зависит от количества упоминаний конкретных угроз (рис. 1–4).

Результаты количественного контент-анализа корпуса документов в сфере ИКТ-безопасности в контексте связей США со странами Латинской Америки можно интерпретировать следующим образом.

Именно четыре державы — Россия, Китай, Иран и КНДР — подаются реципиенту, то есть латиноамериканским странам в качестве основных источников угроз в ИКТ-пространстве. Набор конкретных ассоциаций, связанных с угрозами в области ИКТ-безопасности, представляется достаточно разнообразным. Всем четырем государственным акторам приписываются кибератаки и использование вирусов-вымогателей, трем государствам за исключением КНДР — агрессивные разведывательные операции, кибероперации и угрозы цифровой инфраструктуре в целом. Наконец, трем странам за вычетом Ирана атрибутируется деятельность по кибершпионажу.

Обращает на себя особое внимание тот факт, что администрация Дж. Байдена рассматривала в качестве максимально серьезной угрозы стремление КНР к превосходству в ИКТ-сфере. Второй по важности угрозой оказывается Россия в связи с ее намерением усилить свой ИКТ-потенциал и подорвать влияние США. Соответственно, деятельность китайских и российских компаний на IT-рынках Латиноамериканского региона, в частности при предоставлении услуг в сфере ИКТ-безопасности, трактуется как нежелательная.

*Таблица 1*. **Образная система в дискурсе США в области ИКТ-безопасности**

| Образ | Референция | Предикация |
|---|---|---|
| США как *агент* | – Глобальный лидер в ИКТ<br>– Защитник свободы и демократии<br>– Арбитр в ИКТ-пространстве<br>– Наиболее привлекательный партнер в ИКТ-пространстве<br>– Надежный поставщик ИКТ-безопасности | – Проводит политику по сохранению мирового порядка, основанного на правилах<br>– Отстаивает либеральные ценности<br>– Устанавливает международные нормы в ИКТ-пространстве<br>– Использует ИКТ в благих целях<br>– Заинтересован в сотрудничестве<br>– Намерен помогать партнерам<br>– Стремится укрепить многосторонние институты<br>– Стремится обеспечить честную конкуренцию с учетом своих интересов<br>– Стремится обеспечить коллективную безопасность |
| Латинская Америка как *реципиент* | – Регион с высоким уровнем уязвимости в ИКТ-пространстве<br>– Регион с низким уровнем развития ИКТ<br>– Зависимый от внешней помощи<br>– Преимущественно пассивный партнер | – Нуждается в патернализме со стороны США<br>– Нуждается в помощи для обеспечения ИКТ-безопасности<br>– Нуждается в ресурсах для развития ИКТ<br>– Вносит вклад в коллективную ИКТ-безопасность |
| Китай как *объект* | – Нелиберальное государство<br>– Стратегический конкурент<br>– Наиболее серьезная угроза для США и стран Латинской Америки<br>– Системная угроза<br>– Источник дестабилизации в политике, экономике и ИКТ-пространстве | – Проводит ревизионистскую политику<br>– Стремится превзойти США в ИКТ-пространстве<br>– Продвигает цифровой авторитаризм<br>– Использует ИКТ для достижения агрессивных целей<br>– Подрывает международные нормы<br>– Способен совершать серьезные кибератаки<br>– Нарушает права человека с использованием ИКТ |
| Россия как *объект* | – Нелиберальное государство<br>– Тактический конкурент<br>– Значимая угроза для интересов США в отдельных латиноамериканских странах<br>– Источник дестабилизации в политике, экономике и ИКТ-пространстве | – Проводит ревизионистскую политику<br>– Совершенствует ИКТ-потенциал для расширения вредоносной деятельности против США и их союзников<br>– Осуществляет дезинформацию и пропаганду<br>– Использует ИКТ для достижения агрессивных целей<br>– Подрывает международные нормы<br>– Нарушает права человека с использованием ИКТ |
| КНДР как *объект* | – Нелиберальное государство<br>– Ограниченная угроза для США и их союзников, включая страны Латинской Америки<br>– Источник дестабилизации в политике, экономике и ИКТ-пространстве | – Проводит ревизионистскую политику<br>– Расширяет масштаб вредоносной деятельности в ИКТ-пространстве<br>– Использует ИКТ для достижения агрессивных целей<br>– Получает доходы от преступной деятельности с использованием ИКТ<br>– Нарушает права человека с использованием ИКТ |
| Иран как *объект* | – Нелиберальное государство<br>– Ограниченная угроза для США и их союзников, включая страны Латинской Америки<br>– Источник дестабилизации в политике, экономике и ИКТ-пространстве | – Проводит ревизионистскую политику;<br>– Расширяет масштаб вредоносной деятельности в ИКТ-пространстве<br>– Использует ИКТ для достижения агрессивных целей<br>– Нарушает права человека с использованием ИКТ |

*Примечание.* Основным критерием классификации угроз является коннотативная окраска объектов секьюритизации в рамках рассматриваемого дискурса.

*Источник:* составлено Л.М. Сокольщиком, И.О. Яникеевой и Г.В. Торопчиным на основе контент-анализа собранной базы данных.

*Таблица 2*. **Атрибутируемые государственным акторам угрозы по количеству упоминаний**

| Угроза | Россия | Китай | Иран | КНДР |
|---|---|---|---|---|
| Агрессивные разведывательные операции | 1 | 1 | 1 | – |
| Вирусы-вымогатели | 2 | 1 | 1 | 2 |
| Вредоносное программное обеспечение | – | – | 1 | – |
| Дезинформация | 2 | 1 | – | – |
| Дестабилизирующие киберинструменты | 2 | – | – | – |
| Кибератаки | 3 | 2 | 1 | 2 |
| Кибервлияние | 3 | – | – | – |
| Кибероперации | 1 | 1 | 2 | – |
| Киберпреступления | – | – | – | 2 |
| Киберсбои | 1 | – | – | – |
| Киберугроза (в целом) | 4 | 4 | 1 | – |
| Кибершпионаж | 3 | 2 | – | 2 |
| Манипуляция информацией | 1 | – | – | – |
| Операции по влиянию | – | 1 | – | – |
| Попытки стереть данные | 1 | – | – | – |
| Присвоение киберинфраструктуры | – | – | – | 1 |
| Присвоение криптовалюты | – | – | – | 1 |
| Угроза технологической конкурентоспособности | – | 4 | – | – |
| Цифровой авторитаризм | – | 2 | – | – |

*Источник:* составлено Л.М. Сокольщиком, И.О. Яникеевой и Г.В. Торопчиным на основе контент-анализа собранной базы данных.

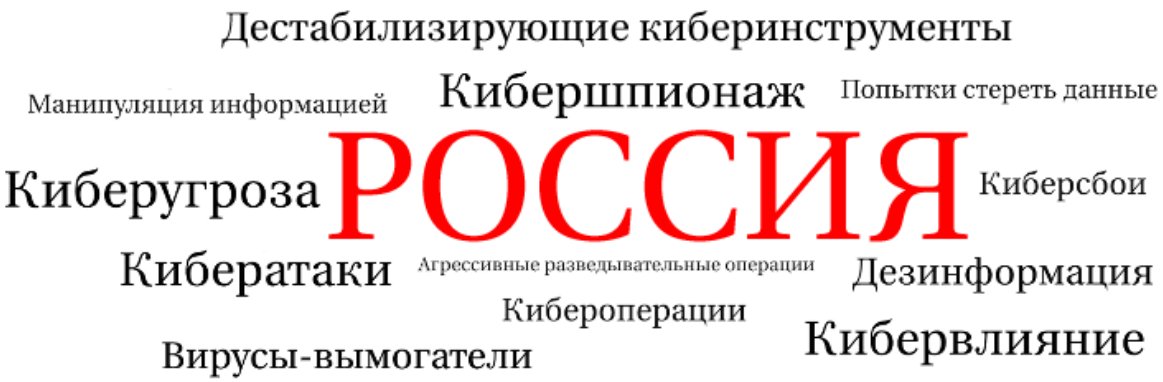


**Рис. 1. Угрозы в сфере ИКТ-безопасности, атрибутируемые России:**
кегль находится в прямой зависимости от количества упоминаний
*Источник:* составлено Г.В. Торопчиным на основе данных из табл. 2.


**Рис. 2. Угрозы в сфере ИКТ-безопасности, атрибутируемые Китаю:**
кегль находится в прямой зависимости от количества упоминаний
*Источник:* составлено Г.В. Торопчиным на основе данных из табл. 2.

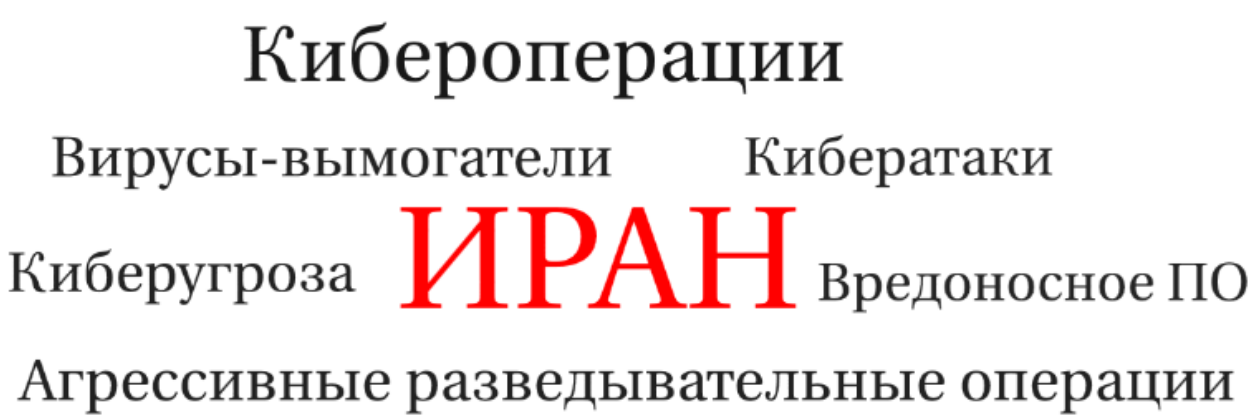


**Рис. 3. Угрозы в сфере ИКТ-безопасности, атрибутируемые Ирану:**
кегль находится в прямой зависимости от количества упоминаний
*Источник:* составлено Г.В. Торопчиным на основе данных из табл. 2.


**Рис. 4. Угрозы в сфере ИКТ-безопасности, атрибутируемые КНДР:**
кегль находится в прямой зависимости от количества упоминаний
*Источник:* составлено Г.В. Торопчиным на основе данных из табл. 2.

При этом ИКТ-угрозы, приписываемые России, в документах неоднократно связываются с проведением специальной военной операции на Украине, что подтверждает вывод об использовании идеологической аргументации при продвижении американских ИКТ в Латинской Америке.

## Заключение

Критический анализ дискурса администрации Дж. Байдена в области ИКТ-безопасности позволил выявить механизмы реализации скрытой идеологии доминирования США в отношении Латинской Америки. Исследование показало, что официальный дискурс играет центральную роль в легитимации гегемонистских устремлений США, представляя их как направленные на защиту демократических ценностей и обеспечение глобальной стабильности. Когнитивная модель контекстного «поля», представленная в американском дискурсе, отражает стремление США сохранить лидерство в глобальном ИКТ-пространстве, укрепляя свои позиции через многосторонние институты и региональное сотрудничество, одновременно противодействуя влиянию других крупных держав, в первую очередь Китая и России, через конструирование образа Вашингтона как исключительного поставщика международной ИКТ-безопасности.

США, выстраивая образную систему «агент — реципиент — объект» через дискурсивные стратегии референции, предикации и аргументации, стремятся оправдать свою активную роль в Латинской Америке, закрепить пассивную позицию латиноамериканских стран, а также легитимизировать

дискриминированное положение Китая, России, Ирана и КНДР как в сфере ИКТ в целом, так и в качестве акторов в Латинской Америке. При этом подобный дискурсивный конструкт обосновывает возможность и даже необходимость вмешательства США в региональные и внутриполитические процессы в области ИКТ-безопасности. Несмотря на то, что в американском дискурсе присутствует стремление к обоснованию данной образной системы технологическими, экономическими, ценностными и альтруистическими аргументами, в конечном счете она оказывается политически мотивирована, а риторика о сотрудничестве во многом лишь вуалирует продвижение американских стратегических интересов в регионе.

Важным направлением для будущих исследований является анализ восприятия дискурса США в области ИКТ-безопасности в странах Латинской Америки. Изучение того, как региональные акторы интерпретируют и реагируют на него, поможет более глубоко понять процесс международного взаимодействия в этой сфере. Кроме того, перспективным является исследование альтернативных моделей международного ИКТ-пространства и его безопасности. Необходимо также углубленное изучение роли других крупных акторов, таких как Евросоюз, Китай и Россия, в формировании политики в области ИКТ-безопасности в Латиноамериканском регионе, чтобы выявить более широкий контекст для анализа.

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

## Список литературы

*Зиновьева Е., Игнатов А.* БРИКС в глобальном режиме ИКТ-безопасности // Международные процессы. 2023. Т. 21, № 4. С. 104–132. https://doi.org/10.17994/IT.2023.21.4.75.2; EDN: AVLWZW

*Крутских А. В.* Международная информационная безопасность: в поисках консолидированных подходов : интервью с Андреем Владимировичем Крутских, Специальным представителем Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности / интервью провел Д. А. Пискунов // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 342–351. https://doi.org/10.22363/2313-0660-2022-22-2-342-351; EDN: DVBISA

*Пахалюк К. А.* Истоки дискурсивного подхода в политических исследованиях // Вестник Московского университета. Серия 18. Социология и политология. 2018. Т. 24, № 1. С. 71–97. https://doi.org/10.24290/1029-3736-2018-24-1-71-97; EDN: YUPBIH

*Понька Т. И., Рамич М. С., У Ю.* Информационная политика и информационная безопасность КНР: развитие, подходы и реализация // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2020. Т. 20, № 2. С. 382–394. https://doi.org/10.22363/2313-0660-2020-20-2-382-394; EDN: UANODL

*Свирчевский Д. А., Фомин И. В.* Образы Европы в дискурсе левых и правых популистов Германии: между Европой солидарности и Европой-крепостью // Полис. Политические исследования. 2023. № 2. С. 27–40. https://doi.org/10.17976/jpps/2023.02.03; EDN: YGNOEA

*Сокольщик Л. М., Сакаев В. Т., Галимуллин Э. З.* Нелегальная иммиграция из Латинской Америки в контексте президентской кампании в США 2024 г.: эффекты поляризации // Международная аналитика. 2023. Т. 14, № 3. С. 106–126. https://doi.org/10.46272/2587-8476-2023-14-3-106-126; EDN: FTAYME

*Сокольщик Л. М., Сокольщик Ю. С., Теремецкий К. С.* Дискурсивные стратегии легитимации санкционной политики США в отношении России (2021–2023) // Полис. Политические исследования. 2024. № 3. С. 109–125. https://doi.org/10.17976/jpps/2024.03.08; EDN: NTYWXM

*Стадник И. Т.* Как изучать политику безопасности в области ИКТ: возможности и ограничения критического дискурс-анализа // Вестник Санкт-Петербургского университета. Международные отношения. 2024. Т. 17, № 2. С. 183–200. https://doi.org/10.21638/spbu06.2024.205; EDN: NKMILI

*Фомин И. В.* Возможности анализа репрезентаций государственных образований в политических дискурсах (на примере образа Косова) // Полис. Политические исследования. 2014a. № 2. С. 124–137. https://doi.org/10.17976/jpps/2014.02.09; EDN: RXHOPN

*Фомин И. В.* Категория образа как средство изучения политической действительности (на примере образа Южной Осетии в российском внешнеполитическом дискурсе) // Символическая политика : сборник статей. Вып. 2.: Споры о прошлом как проектирование будущего. Москва : Институт научной информации по общественным наукам РАН, 2014b. С. 40–65. EDN: ULCLXR

*Хейфец В. Л., Хадорич Л. В.* Латинская Америка между ОАГ и СЕЛАК // Мировая экономика и международные отношения. 2015. № 4. С. 90–100. https://doi.org/10.20542/0131-2227-2015-4-90-100; EDN: TRNTVZ

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

*Buzan B., Wæver O., de Wilde J.* Security: A New Framework for Analysis. London : Boulder, Lynne Rienner Publishers, 1998. URL: https://www.academia.edu/39047709/Buzan_Waever_and_De_Wilde_1998_Security_A_New_Framework_For_Analysis (accessed: 14.01.2025)

*Campbell D.* Politics Without Principle : Sovereignty, Ethics, and the Narratives of the Gulf War. Boulder, USA : Lynne Rienner Publishers, 1993. https://doi.org/10.1515/9781685856090

*Henshaw A.* Capacity Building and Cyber Insecurity in Latin America: Geopolitics, Surveillance, and Disinformation // Critical Perspectives on Cybersecurity : Feminist and Postcolonial Interventions / ed. by A. Mhajne, A. Henshaw. New York : Oxford University Press, 2024. P. 173–193. https://doi.org/10.1093/oso/9780197695883.003.0008

*Hurel L. M.* Interrogating the Cybersecurity Development Agenda: A Critical Reflection // The International Spectator. 2022. Vol. 57, iss. 3. P. 66–84. https://doi.org/10.1080/03932729.2022.2095824; EDN: SPVBPZ

*Krebs R. R.* How Dominant Narratives Rise and Fall: Military Conflict, Politics, and the Cold War Consensus // International Organization. 2015. Vol. 69, iss. 4. P. 809–845. https://doi.org/10.1017/S0020818315000181

*Miao W., Xu J., Zhu H.* From Technological Issue to Military-Diplomatic Affairs: Analysis of China's Official Cybersecurity Discourse (1994–2016) // Second International Handbook of Internet Research / ed. by J. Hunsinger, M. Allen, L. Klastrup. Dordrecht : Springer, 2019. P. 1–13. https://doi.org/10.1007/978-94-024-1202-4_61-1

*Reisigl M., Wodak R.* The Discourse-Historical Approach (DHA) // Methods of Critical Discourse Analysis : 2nd revised edition / ed. by R. Wodak, M. Meyer. London: SAGE, 2009. URL: https://www.researchgate.net/publication/251636976_The_Discourse-Historical_Approach_DHA (accessed: 14.01.2025).

*Siudak R.* Cybersecurity Discourses and Their Policy Implications // Journal of Cyber Policy. 2022. Vol. 7, iss. 3. P. 318–335. https://doi.org/10.1080/23738871.2023.2167607; EDN: MLSWMA

*Sokolshchik L. M.* Year One of the Biden Administration: U.S. Foreign Policy Towards Russia // Journal of Eurasian Studies. 2024. Vol. 15, iss. 1. P. 70–80. https://doi.org/10.1177/18793665231170639; EDN: AMHXNS

*Sokolshchik L., Sokolshchik Y.* Why U.S. — Russia Relations Failed: An Analysis of Competing National Security Narratives // Russian Politics. 2023. Vol. 8, no. 4. P. 468–492. https://doi.org/10.30965/24518921-00803009; EDN: YFYVMB

*Tikk E., Kerttunen M.* Introduction // Routledge Handbook of International Cybersecurity / ed. by E. Tikk, M. Kerttunen. New York : Routledge, 2020. P. 1–8. https://doi.org/10.4324/9781351038904

*Urbanovics A.* Cybersecurity Policy-Related Developments in Latin America // AARMS — Academic and Applied Research in Military and Public Management Science. 2022. Vol. 21, no. 1. P. 79–94. https://doi.org/10.32565/aarms.2022.1.6; EDN: JOBKFG

*Van Dijk T. A.* Discourse, Context and Cognition // Discourse Studies. 2006. Vol. 8, iss. 1. P. 159–177. https://doi.org/10.1177/1461445606059565

*Wendt A.* Social Theory of International Politics. Cambridge : Cambridge University Press, 1999. https://doi.org/10.1017/CBO9780511612183

**Сведения об авторах:**

*Сокольщик Лев Маркович* — кандидат исторических наук, ведущий научный сотрудник, Центр комплексных европейских и международных исследований, Национальный исследовательский университет «Высшая школа экономики»; Российская Федерация, 119017, г. Москва, ул. Малая Ордынка, д. 17; eLibrary SPIN-код: 6958-8932; ORCID: 0000-0002-0945-1022; e-mail: lsokolshchik@hse.ru

*Яникеева Инна Олеговна* — кандидат политических наук, научный сотрудник, Центр комплексных европейских и международных исследований, Национальный исследовательский университет «Высшая школа экономики»; Российская Федерация, 119017, г. Москва, ул. Малая Ордынка, д. 17; eLibrary SPIN-код: 5148-7454; ORCID: 0000-0001-9590-5301; e-mail: iyanikeeva@hse.ru

*Торопчин Глеб Вячеславович* — кандидат исторических наук, заместитель декана по научной работе, факультет гуманитарного образования, Новосибирский государственный технический университет; Российская Федерация, 630073, г. Новосибирск, проспект К. Маркса, д. 20; старший научный сотрудник, Центр евразийских исследований, Национальный исследовательский Томский государственный университет; Российская Федерация, 634050, г. Томск, проспект Ленина, 36; eLibrary SPIN-код: 1524-2434; ORCID: 0000-0002-8055-1202; e-mail: glebtoropchin@mail.ru