

УДК 32**Кибердипломатия как направление внешней политики США****Ротаренко Антон Дмитриевич**

Аспирант,
Воронежский филиал,
Российская академия народного хозяйства
и государственной службы при Президенте РФ,
394005, Российская Федерация, Воронеж, Московский пр., 143;
e-mail: kafppu@vnp.ranepa.ru

Аннотация

Кибердипломатия, превратившись в важное направление внешней политики США, призвана обеспечивать национальные интересы и продвигать американские ценности в цифровом мире. В статье исследуется арсенал инструментов, используемых США для достижения этих целей, включая дипломатические переговоры, экономические санкции, техническую помощь и кибероперации. Особое внимание уделяется вызовам, связанным с конкуренцией между государствами и отсутствием общепринятых норм. Подчеркивается необходимость постоянной адаптации стратегий и подходов кибердипломатии США к быстро меняющемуся цифровому ландшафту для эффективного противодействия новым угрозам.

Для цитирования в научных исследованиях

Ротаренко А.Д. Кибердипломатия как направление внешней политики США // Теории и проблемы политических исследований. 2025. Том 14. № 3А. С. 49-55.

Ключевые слова

Кибердипломатия, информационное пространство, международные отношения.

Введение

В эпоху цифровой трансформации, когда киберпространство пронизывает все сферы жизни – от экономики и политики до безопасности и межличностных отношений, вопросы кибербезопасности и международного сотрудничества в цифровой сфере приобретают первостепенное значение. Киберпространство, ставшее ареной для беспрецедентных возможностей, одновременно породило и новые угрозы, такие как кибершпионаж, киберпреступность и кибервойны, ставящие под вопрос стабильность и безопасность государств. В этих условиях, кибердипломатия, как новый инструмент внешней политики, становится ключевым элементом в обеспечении глобальной стабильности и безопасности.

Кибердипломатия – это многогранный подход к управлению международными отношениями в киберпространстве. Она охватывает широкий спектр деятельности, направленной на предотвращение конфликтов, содействие сотрудничеству и защиту национальных интересов в цифровой сфере. Разные страны и организации могут иметь разные взгляды на то, что входит в понятие кибердипломатии. Некоторые аспекты кибердипломатии, такие как киберразведка, до сих пор вызывают споры и разногласия. Также специалисты выделяют такие аспекты как, кибербезопасность, киберпреступность, цифровая экономика, цифровая дипломатия, свобода интернета и др. [Painter, 2020]

Хотя данное направление и весьма молодое, тем не менее специалисты уже выделяют определённые этапы эволюции кибердипломатии:

- Ранний этап (1990-е – начало 2000-х): осознание потенциала интернета для дипломатии, использование электронной почты и веб-сайтов;
- Этап развития (середина 2000-х – начало 2010-х): распространение социальных сетей, рост киберпреступности и первые международные соглашения;
- Этап зрелости (с начала 2010-х по настоящее время): признание киберпространства новым театром действий, увеличение кибератак и активное развитие кибердипломатии. [Painter, 2018]

Основная часть

Развитие кибердипломатии в США – это динамичный процесс, отражающий растущее значение киберпространства в международных отношениях. Рассматривая роль США в развитии кибердипломатии, можно увидеть, как с годами менялся их подход в этом вопросе.

Ранние годы (1990-е – начало 2000-х):

Фокус на кибербезопасности: первоначально усилия США были сосредоточены на защите собственной критической инфраструктуры от кибератак. Можно наблюдать как создавались специализированные подразделения: в правительстве США появились подразделения, занимающиеся вопросами кибербезопасности, такие как Computer Emergency Readiness Team (CERT).

Середина 2000-х – начало 2010-х:

США начали рассматривать киберпространство как потенциальное поле боя и разрабатывать стратегии для ведения кибервойны. Сразу же начались конкретные шаги, такие как создание командования Cyber Command в 2010 году (USCYBERCOM), отвечающее за кибероперации в вооруженных силах США. США начали участвовать в международных

инициативах по кибербезопасности, таких как Будапештская конвенция о киберпреступности и др.

С начала 2010-х по настоящее время:

Кибердипломатия становится одним из приоритетов внешней политики США. Госдепартамент США начинает играть ключевую роль в кибердипломатии, занимаясь ведением переговоров, разработкой международных норм и продвижением свободы интернета. В структуре Госдепартамента появилось Бюро по киберпространству и цифровой политике (Bureau of Cyberspace and Digital Policy, CDIP), которое так сформулировало свои задачи: «Бюро по киберпространству и цифровой политике (CDP) содействует национальной и экономической безопасности США, возглавляя, координируя и повышая значимость внешней политики в области киберпространства и цифровых технологий. Оно налаживает партнерские отношения для формирования международной среды, чтобы американцы и люди во всем мире могли процветать. CDP стремится к миру, в котором каждый человек может получить доступ к возможностям, предоставляемым цифровой связью, для построения процветающих экономик и обществ, и работает над противодействием вызовам этому видению со стороны авторитарных государств». [Carlson, 2024]

Невозможно не отметить и другие не менее важные аспекты развития кибердипломатии в США в эти годы: разрабатывается ряд национальных стратегий кибербезопасности; наращивается активное сотрудничество со своими союзниками по НАТО и другими странами в области кибербезопасности и кибердипломатии; уделяется большое внимание противодействию иностранному вмешательству в свои выборы и политические процессы через киберпространство.

Развитие кибердипломатии в США ознаменовалось несколькими ключевыми моментами. Во-первых, произошло осознание киберпространства как стратегического актива, который необходимо защищать, и одновременно - как потенциальной угрозы, требующей постоянного внимания и адекватного ответа. Во-вторых, кибердипломатия была интегрирована в общую внешнюю политику США, став неотъемлемой частью стратегии продвижения национальных интересов на международной арене. В-третьих, США активно продвигают свои ценности, такие как свобода слова и открытый интернет, в киберпространстве, стремясь сформировать его в соответствии со своими идеалами. В-четвертых, для сдерживания киберугроз США сочетают дипломатические усилия с военным потенциалом, демонстрируя готовность использовать различные инструменты для защиты своих интересов. И наконец, США делают упор на многостороннее сотрудничество с союзниками и партнерами, признавая, что эффективная кибердипломатия требует консолидированных усилий международного сообщества.

Несмотря на значительные успехи, кибердипломатия США сталкивается с рядом серьезных вызовов. Во-первых, отсутствие общепринятых международных норм поведения в киберпространстве затрудняет достижение согласия относительно правил игры и создает почву для конфликтов.

Во-вторых, сложность атрибуции кибератак, то есть установления их источника, подрывает доверие и затрудняет привлечение виновных к ответственности. В-третьих, поддержание баланса между обеспечением кибербезопасности и защитой фундаментальных ценностей, таких как свобода слова и конфиденциальность в интернете, представляет собой непростую задачу, требующую деликатного подхода. И, наконец, растущая конкуренция с другими крупными державами, такими как Китай и Россия, в киберпространстве требует от США постоянного совершенствования своих стратегий и инструментов кибердипломатии. [Kuznetsov, Liang, 2023]

В качестве примеров успешных кибердипломатических усилий США можно привести несколько направлений. Во-первых, США активно поддерживают свободу интернета и стремятся помочь гражданам стран с авторитарными режимами обходить цензуру. Это выражается в финансировании разработки и распространения инструментов обхода цензуры, таких как Tor, Psiphon и Lantern, а также в поддержке независимых СМИ и правозащитных организаций. U.S. Agency for Global Media (USAGM), управляющее международными вещательными организациями, такими как Voice of America и Radio Free Europe/Radio Liberty, играет важную роль в распространении информации и противодействии дезинформации. Во-вторых, США активно сотрудничают с НАТО в области кибербезопасности, участвуя в совместных учениях, обмене информацией и разработке общих стратегий.

В частности, участие в учениях Locked Shields, крупнейших в мире международных учениях по кибербезопасности, организованных НАТО Cooperative Cyber Defence Centre of Excellence (CCDCOE), позволяет повысить уровень кибербезопасности НАТО и готовность союзников к отражению кибератак. [Shepperd, 2024]

Наряду с успехами, в кибердипломатии США существуют и спорные моменты, которые иллюстрируют сложности и противоречия, возникающие при реализации внешней политики в киберпространстве. Так, долгое время США подвергались критике за свою роль в управлении ICANN (Internet Corporation for Assigned Names and Numbers), организацией, контролирующей ключевые аспекты функционирования интернета, такие как доменные имена и IP-адреса. Хотя впоследствии США отказались от прямого контроля над ICANN, критика их роли в глобальном управлении интернетом не исчезла полностью. [6] Другим спорным моментом является использование кибероружия. Обвинения в адрес США в применении кибероружия против других стран, включая Иран (Stuxnet) и Россию, поднимают вопросы о соблюдении международного права и рисках эскалации конфликтов в киберпространстве. Факт применения кибероружия подрывает их авторитет как приверженца мирного урегулирования споров. Наконец, вызывает вопросы и недостаточная защита персональных данных американских граждан. Отсутствие единого федерального закона о защите персональных данных создает уязвимости для утечек информации и киберпреступлений, что подрывает доверие к цифровой экономике и ставит под угрозу безопасность граждан.

Для реализации кибердипломатических целей США используют широкий спектр инструментов, которые условно можно разделить на несколько категорий. К дипломатическим инструментам относятся, прежде всего, переговоры и диалог – как на двусторонней основе, например, с Россией и Китаем, несмотря на существующую политическую напряженность, так и в многостороннем формате. Также используются соглашения и меморандумы о взаимопонимании (MoU) с различными странами, формализующие сотрудничество в сфере кибербезопасности. Важную роль играет публичная дипломатия и информационная деятельность, направленная на продвижение американских ценностей и политики в киберпространстве, противодействие дезинформации и повышение осведомленности о киберугрозах посредством публичных выступлений высокопоставленных чиновников и активного использования социальных сетей Государственным департаментом и американскими посольствами. Другая категория – экономические инструменты, включающие в себя санкции, применяемые к лицам, организациям и странам, причастным к киберпреступлениям, кибершпионажу и другим злонамеренным действиям. Экспортный контроль ограничивает вывоз технологий и программного обеспечения, технологий разработки искусственного интеллекта или программного обеспечения для взлома паролей. Наконец, стимулирование инвестиций в кибербезопасность создает благоприятные условия для

развития отрасли, включая государственные программы поддержки малого и среднего бизнеса и инвестиции в исследования и разработки.

Помимо дипломатических и экономических инструментов, важную роль играют технические инструменты, включающие оказание технической помощи другим странам для наращивания их потенциала в области кибербезопасности. Это выражается в обучении специалистов, предоставлении оборудования и программного обеспечения, а также консультировании по разработке национальных стратегий, примером чего являются программы обучения специалистов из развивающихся стран и техническая помощь Украине в защите от кибератак. Важным элементом является обмен информацией о киберугрозах с другими странами и частным сектором. Наконец, США не исключают применение военных инструментов, а именно проведение киберопераций, для сдерживания агрессии, защиты критической инфраструктуры и поддержки военных операций в реальном мире. Примером может служить официально признанное проведение киберопераций против ИГИЛ (запрещенная в РФ организация) для подрыва их пропагандистской деятельности и финансовой инфраструктуры. Предполагаемое участие США в разработке и применении вируса Stuxnet против иранских ядерных объектов, хотя и не подтверждено официально, также иллюстрирует возможность использования подобных мер. [Fruhlinger, 2022]

Заключение

В перспективе, кибердипломатия США, по всей видимости, будет развиваться по нескольким ключевым направлениям. Вероятно усиление акцента на сдерживании и обороне киберугроз, что предполагает увеличение инвестиций в соответствующие возможности, укрепление сотрудничества с союзниками, разработку новых видов кибервооружений и повышение уровня защиты критической инфраструктуры. Важную роль продолжит играть многосторонняя дипломатия, направленная на укрепление механизмов сотрудничества в рамках ООН, НАТО, ОБСЕ и других международных организаций. [Peters, 2020] США, вероятно, не откажутся от активного продвижения демократических ценностей, таких как свобода слова и открытый интернет, оказывая поддержку проектам, направленным на обход цензуры, защиту независимых СМИ и противодействие дезинформации. Борьба с киберпреступностью останется одним из приоритетов, что предполагает расширение сотрудничества с другими странами. Цифровая дипломатия, использующая социальные сети и онлайн-платформы, будет и далее применяться для продвижения интересов и ценностей США за рубежом. Учитывая значительную роль частного сектора в киберпространстве, можно ожидать углубления сотрудничества государства и частных компаний. Возрастет внимание к регулированию новых технологий, таких как искусственный интеллект и блокчейн. Наконец, США будут инвестировать в развитие кадрового потенциала, обучая и подготавливая специалистов в области кибердипломатии и кибербезопасности. [Sabin, 2024]

Эволюционировав в одно из ключевых направлений внешней политики США, сейчас кибердипломатия представляет собой комплексный подход к управлению вызовами и возможностями цифрового мира. Используя разнообразный инструментарий, от традиционной дипломатии до технических средств и мер экономического воздействия, США будут продолжать защищать свои интересы, продвигая демократические ценности и обеспечивая стабильность в киберпространстве, чтобы в полной мере противостоять возникающим угрозам и использовать потенциал цифровой эпохи. [Vasiloiu, 2023]

Библиография

1. CHRIS PAINTER, "The rise of the internet and cyber technologies constitutes one of the central foreign policy issues of the 21st century." // *Procedia Computer Science*. 2020, vol. 176, pp. 60–69. URL: <https://doi.org/10.1016/j.procs.2020.08.007>.
2. CHRIS PAINTER, "The rise of the internet and cyber technologies constitutes one of the central foreign policy issues of the 21st century." // *The Foreign Service Journal*. 2018. URL: <https://afsa.org/diplomacy-cyberspace>.
3. Brian Carlson. "What is The CDP Bureau?". // *The Customer data platform resource*, 2024. URL: <https://cdp.com/articles/what-is-the-cdp-bureau/>.
4. Kuznetsov N.M., Fushu Liang. "Digital diplomacy of USA and China in the era of datalization". // *Vestnik of Saint Petersburg University. International Relations*, 2023, vol. 16, issue 2, pp. 191–200. URL: <https://doi.org/10.21638/spbu06.2023.206>.
5. James Shepperd. "Locked Shields 2024: Ancient inspiration deployed for today's complex digital battlegrounds". // *ESET Blog*, 2024. URL: <https://www.eset.com/blog/company/locked-shields-2024-ancient-inspiration-deployed-for-todays-complex-digital-battlegrounds/>.
6. Rick Lane. "The Crisis of ICANN's Failed Internet Governance". // *Medium*, 2022. URL: <https://medium.com/@rick.lane22/the-crisis-of-icanns-failed-internet-governance-1684d789de33>.
7. Josh Fruhlinger. "Stuxnet explained: The first known cyberweapon". // *CSO*, 2022. URL: <https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html>.
8. Allison Peters. "US Global Cybercrime Cooperation: A Brief Explainer". // *THIRD WAY*, 2020. URL: *US Global Cybercrime Cooperation: A Brief Explainer – Third Way*
9. Sam Sabin. "State Department unveils roadmap for cyber diplomacy". // *AXIOS*, 2024. URL: *State Department unveils new international strategy for cyber diplomacy*
10. Ioana-Cristina Vasiloiu. "Comparative Analysis on Cyber Diplomacy in EU and US". // *ACADEMIA*, 2023. URL: *Comparative Analysis on Cyber Diplomacy in EU and US*

Cyberdiplomacy as a Direction of US Foreign Policy

Anton D. Rotarenko

Postgraduate Student,
Voronezh Branch,
Russian Presidential Academy
of National Economy and Public Administration,
394005, 143, Moskovskiy ave., Voronezh, Russian Federation;
e-mail: kafppu@vm.ranepa.ru

Abstract

Cyberdiplomacy has become an important direction of US foreign policy, aimed at ensuring national interests and promoting American values in the digital world. The article examines the arsenal of tools used by the United States to achieve these goals, including diplomatic negotiations, economic sanctions, technical assistance, and cyber operations. Particular attention is paid to the challenges associated with interstate competition and the lack of universally accepted norms. The study emphasizes the need for constant adaptation of US cyberdiplomacy strategies and approaches to the rapidly changing digital landscape to effectively counter emerging threats.

For citation

Rotarenko A.D. (2025) Kiberdiplomatiya kak napravlenie vneshney politiki SShA [Cyberdiplomacy as a Direction of US Foreign Policy]. *Teorii i problemy politicheskikh issledovaniy* [Theories and Problems of Political Studies], 14 (3A), pp. 49-55.

Rotarenko A.D.

Keywords

Cyberdiplomacy, information space, international relations.

References

1. CHRIS PAINTER, "The rise of the internet and cyber technologies constitutes one of the central foreign policy issues of the 21st century." // *Procedia Computer Science*. 2020, vol. 176, pp. 60–69. URL: <https://doi.org/10.1016/j.procs.2020.08.007>.
2. CHRIS PAINTER, "The rise of the internet and cyber technologies constitutes one of the central foreign policy issues of the 21st century." // *The Foreign Service Journal*. 2018. URL: <https://afsa.org/diplomacy-cyberspace>.
3. Brian Carlson. "What is The CDP Bureau?". // *The Customer data platform resource*, 2024. URL: <https://cdp.com/articles/what-is-the-cdp-bureau/>.
4. Kuznetsov N.M., Fushu Liang. "Digital diplomacy of USA and China in the era of datalization". // *Vestnik of Saint Petersburg University. International Relations*, 2023, vol. 16, issue 2, pp. 191–200. URL: <https://doi.org/10.21638/spbu06.2023.206>.
5. James Shepperd. "Locked Shields 2024: Ancient inspiration deployed for today's complex digital battlegrounds". // *ESET Blog*, 2024. URL: <https://www.eset.com/blog/company/locked-shields-2024-ancient-inspiration-deployed-for-todays-complex-digital-battlegrounds/>.
6. Rick Lane. "The Crisis of ICANN's Failed Internet Governance". // *Medium*, 2022. URL: <https://medium.com/@rick.lane22/the-crisis-of-icanns-failed-internet-governance-1684d789de33>.
7. Josh Fruhlinger. "Stuxnet explained: The first known cyberweapon". // *CSO*, 2022. URL: <https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html>.
8. Allison Peters. "US Global Cybercrime Cooperation: A Brief Explainer". // *THIRD WAY*, 2020. URL: *US Global Cybercrime Cooperation: A Brief Explainer – Third Way*
9. Sam Sabin. "State Department unveils roadmap for cyber diplomacy". // *AXIOS*, 2024. URL: *State Department unveils new international strategy for cyber diplomacy*
10. Ioana-Cristina Vasiloiu. "Comparative Analysis on Cyber Diplomacy in EU and US". // *ACADEMIA*, 2023. URL: *Comparative Analysis on Cyber Diplomacy in EU and US*