УДК 32 **DOI: 10.34670/AR.2022.50.22.028**

Основные угрозы и механизмы обеспечения информационной безопасности государства в сфере публичной дипломатии

Власов Антон Владимирович

Аспирант,
Институт права и национальной безопасности,
Российская академия народного хозяйства
и государственной службы при Президенте РФ,
119571, Российская Федерация, Москва, пр. Вернадского, 84;
e-mail: fst34@mail.ru

Аннотация

Аспект достижения информационной безопасности на национальном уровне в области публичной дипломатии приобретает все более значимую роль в условиях стремительного развития Четвертой промышленной революции, сопровождающейся активным освоением и развитием цифрового пространства. Исследование в данном направлении было проведено с помощью анализа, синтеза, описательного и сравнительного научных методов. В статье рассмотрены подходы достижения информационной безопасности, применяемые государствами в данной сфере, с точки зрения существующих угроз и вызовов, таких, как чрезмерный уровень свободы в Интернете и социальных сетях, устаревание знаний и компетенций в цифровом пространстве, угроза раскрытия информации и потеря секретности, культура анонимности, хакерство. В заключении предлагаются методы обеспечения информационной безопасности в сфере публичной дипломатии в Российской Федерации: активизация участия представителей отечественных технологических предприятий с последующей разработкой программного обеспечения и инструментов цифровой защиты, а также Интернет-краудсорсинг как инструмент своевременного донесения проверенной информации до широкого круга лиц.

Для цитирования в научных исследованиях

Власов А.В. Основные угрозы и механизмы обеспечения информационной безопасности государства в сфере публичной дипломатии // Теории и проблемы политических исследований. 2022. Том 11. № 1А. С. 133-139. DOI: 10.34670/AR.2022.50.22.028

Ключевые слова

Публичная дипломатия, информационная безопасность, цифровое пространство, угрозы информационной безопасности, государство.

Введение

На сегодняшний день глобальное общество живет в эпоху быстрого технологического прогресса: буквально за несколько лет технологии искусственного интеллекта, Интернета вещей и аналитики больших данных вошли не только практически во все сферы политической и экономической деятельности государства, но и в повседневную жизнь человека. В связи с этим особое внимание следует уделить обеспечению информационной безопасности.

Основная часть

Можно выделить три основных подхода, благодаря которым государства формируют и сохраняют безопасность информационного пространства [Psaila, 2021]:

- усиление собственной защиты для подготовки и предотвращения потенциальных киберугроз;
- сдерживание других субъектов (государственных и негосударственных) от участия в заведомо опасной деятельности в сфере анализа, обработки и передачи информации;
- публичная дипломатическая деятельность для отстаивания собственных национальных интересов и ценностей на международной арене.

Обеспечение информационной безопасности в области публичной дипломатии требует понимания технологического потенциала, а также возможных рисков и методов его злоупотребления. За последние годы практика дипломатии распространилась на новые области политики, включая проблемные аспекты, связанные с цифровизацией [Riordan, 2016]. Таким образом, ведение публичной дипломатической деятельности в отношении интересов государства начинает все интенсивнее осуществляться в условиях цифрового пространства, где национальные интересы, как правило, определяются в рамках национальных стратегий развития цифрового пространства и информационной безопасности, а также в контексте внешней политики в области цифровых технологий [Kurbalija, Hone, 2021]. Дополнительным вызовом текущего времени является активное применение цифровых средств, выступающих в качестве инструмента достижения целей в сфере публичной дипломатии [Diplofoundation, www].

Таким образом, актуальными задачами обеспечения информационной безопасности в контексте реализации публичной дипломатической деятельности являются:

- ответственное поведение государств в цифровом пространстве на международной арене и меры укрепления взаимного доверия;
- защита Интернет-пространства и стратегически значимой цифровой инфраструктуры страны;
- предотвращение конфликтов в цифровом пространстве;
- разработка политических мер, касающихся сетевой и информационной безопасности;
- борьба с киберпреступностью и оказание взаимной правовой помощи на межгосударственном уровне;
- разработка и осуществление мер внешней политики в цифровом пространстве.

Решение данных задач требует консолидации усилий на всех уровнях внутри государства [Kasper, Vernygora, 2021]:

- на уровне лиц, ответственных в сфере публичной дипломатии: необходимо повышение знаний и компетенций, включая базовое понимание функционирования Интернета, а также углубленное понимание ключевых вопросов и стратегических целей в области

политической и социально-экономической деятельности государства. Здесь же значимыми являются гибкие навыки ведения переговоров.

- на корпоративном уровне: важно уделить особое внимание вопросам сохранности информации в рамках внешнеполитического курса; для разработки и решения такого рода вопросов требуется консолидация человеческих и финансовых ресурсов. Внутри самих организаций требуется сформировать культуру непрерывного профессионального роста и продвижения по службе посредством повышения квалификации, в том числе благодаря развитию цифровых компетенций.
- на институциональном уровне: следует проводит периодический мониторинг в сфере технических, правовых и экономических аспектов использования цифрового пространства, с последующим применением полученных результатов для разработки институциональной и государственной политики.
- на межнациональном уровне: необходимо формирование стратегического понимания национальных, региональных и глобальных приоритетов государства.

Специалистами выделяются следующие угрозы информационной безопасности, с которыми государства сталкиваются в сфере публичной дипломатии [Pamment, 2016; Renard, 2018; Graham, 2020]:

1) чрезмерный уровень свободы в Интернете и социальных сетях: в настоящее время развитие веб-сайтов министерствами иностранных дел, посольствами и делегациями международных организаций является стандартной практикой. Веб-сайты министерств иностранных дел служат платформой по объяснению и представлению их национальной внешней политики, а также по опровержению неприемлемых действий или претензий других государств (в случае возникновения таковых). Но более открытыми и прозрачными являются аккаунты в социальных сетях.

Информационная глобализация поощряет формирование цифровых связей и взаимодействия, публикацию экспертных и аналитических обзоров с диаметрально противоположными мнениями. Поэтому возможности Интернета далеко не всегда применяют с благими намерениями: террористическими и националистскими организациями осуществляется мобилизация и вербовка сторонников, распространяются идеи экстремизма и навязывания иностранных идеологий. Интернет-площадки способствуют увеличению числа голосов в области разработки международных и внутринациональных политических проектов, что, в свою очередь, ведет к уменьшению внутригосударственного контроля этих процессов.

2) стремительное устаревание знаний и компетенций в цифровом пространстве: на сегодняшний дел министерствам иностранных дел необходимо организовывать своевременное обучение дипломатов эффективному использованию цифровых средств связи, а также назначить лиц, ответственных за анализ и изучение передовых научно-технических достижений [Ruffini, 2017], которые впоследствии уместно внедрить в рамках ведения дипломатической деятельности.

3) угроза раскрытия информации и потери секретности: активное использование интернет-технологий и социальных сетей является прямым вызовом сохранению секретности в публичной дипломатии. Для директивных органов немедленное распространение информации о только произошедшем событии является скорее риском, чем выгодой. К сожалению, уровень коммуникационной культуры в социальных сетях остается на довольно низком уровне и сопровождается ситуациями, когда многие политические лидеры и дипломаты сталкиваются с оскорблениями, а также провокационными и угрожающими посланиями, вызывая тем самым

многочисленные разногласия. Данная область требует скоординированных усилий со стороны органов государственной власти, дипломатов и представителей гражданского общества для нормативно-правового и этического регулирования цифрового пространства.

4) культура анонимности: является еще одной серьезной угрозой информационной безопасности публичной дипломатии. Культура анонимности может привести к возникновению существенных кризисных ситуаций в результате публикации противоречивой, а порой и лживой информации.

5) хакерство: рассматривается в качестве одного из наиболее опасных рисков информационной безопасности в сфере публичной дипломатии. Многие главы государств, представители правительственных и неправительственных организаций, а также дипломаты сталкивались с атаками хакеров, действия которых ставили под угрозу карьеру и миссию. Дипломатические соперники, в том числе государственные и негосударственные организации, предпринимают нередкие попытки по атаке правительственных систем стран для получения конфиденциальной стратегической информации.

В эпоху цифровизации чрезвычайно важным становится реализация методов контроля информации и обеспечения информационной безопасности, и данное направление занимает центральное место в международных дипломатических и политических программах ведущих политических и дипломатических объединений мира.

Касательно ситуации в Российской Федерации, необходимо отметить, что государственные органы с последнего десятилетия прошлого века на регулярной основе разрабатывают предложения по достижению информационной безопасности в сфере публичной дипломатии. Так, в 2011 г. была предложена концепция Конвенции об обеспечении международной информационной безопасности [Демидов, 2013].

В последнее время дипломатические организации Российской Федерации ведут активную деятельность в рамках цифрового пространства, являющегося инструментом продвижения и распространения внешнеполитического курса и роста привлекательности образа государства на международной арене. Примечательно, что в качестве субъектов глобальной информационной среды выступают не только представители государственной власти, но и транснациональные корпорации, организации гражданского общества, сообщества в социальных сетях и физические лица. Таким образом, на публичную дипломатию в рамках цифрового пространства оказывают влияние не только органы государственной власти, но и представители бизнеса и общественные организации.

Одним из приоритетных и перспективных направлений повышения эффективности обеспечения информационной безопасности в сфере публичной дипломатии является разработка мер по активизации участия представителей отечественных технологичных предприятий и повышению популярности разработанного российскими специалистами программного обеспечения и Интернет-платформ. Для русскоязычного населения, проживающего за рубежом, в качестве результативного решения стала бы организация специального информационного портала с целью укрепления взаимодействия с русскоязычными диаспорами, включая профессиональные и научные области.

Интернет-краудсорсинг – еще одна мера, положительно себя зарекомендовавшая для продвижения публичной дипломатии, - представляет собой технологию координации усилий различных членов общества в цифровом пространстве. Она позволяет формировать интерактивные карты угроз и рисков для последующего обсуждения на всех уровня общества, создавать политико-дипломатические сообщества на интерактивной основе, а также

своевременно информировать широкие слои населения в случае наступления кризисных ситуаций.

Заключение

Таким образом, разработка и принятие цифровых инициатив, с одной стороны, может быть рассмотрена в качестве серьезного вызова в сфере публичной дипломатии, поскольку данный процесс радикально изменил развитие дипломатической деятельности, аспект управления и контроля информации, проведение международных переговоров и урегулирование кризисов.

Цифровые технологии чрезвычайно полезны для сбора и обработки информации о дипломатической деятельности, а также для оперативной связи в чрезвычайных ситуациях. Благодаря им для членов общества, живущих в странах с авторитарным режимом, становится возможным избежать ограничений, препятствующих свободному выражению их мнения.

Тем не менее, ведение активной деятельности в цифровом пространстве также несет в себе и существенные угрозы для сферы публичной дипломатии. Свобода в Интернете и социальных сетях, в аккаунтах которых может находиться кто угодно, вызывает множество опасений – это является основной причиной критики цифровых платформ правительствами стран мира, по мнению которых их владельцы недостаточно вовлечены в борьбу с предотвращением экстремизма, терроризма и навязывания антидемократических идеологий.

Для представителей дипломатических организаций отсутствие знаний об использовании цифровых технологий, Интернета и социальных медиа может привести к серьезным негативным последствиям.

В качестве эффективных мер обеспечения информационной безопасности в сфере публичной демократии может выступать развитие отечественных Интернет-площадок и платформ с сохранением данных и цифровой защитой, а также технологий Интернет-краудсорсинга, позволяющая представлять достоверную информацию целевым пользователям.

Библиография

1. Демидов О.В. Обеспечение международной информационной безопасности и российские национальные интересы // Индекс безопасности. 2013. Т. 10. № 1 (104). С. 129-168.
2. DiploFoundation. Digital as a tool for diplomacy. URL: https://www.diplomacy.edu/e-diplomacy#ff1-3
3. Graham S. Online Harms and the Legality Principle. URL: https://www.cyberleagle.com/2020/06/online-harms-and-legality-principle.html
4. Kasper A., Vernigora V. The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market? // DEUSTO Journal of European Studies. 2021. № 65. P. 29-71. DOI https://doi.org/10.18543/ced-65-2021pp29-71
5. Kurbalija J., Hone K. The Emergence of Digital Foreign Policy. 2021. URL: https://www.diplomacy.edu/sites/default/files/2021-03/2021_The_emergence_of_digital_for- eign_policy.pdf
6. Pamment J. British Public Diplomacy and Soft Power: Diplomatic Influence and the Digital Revolution. Palgrave MacMillan, 2016. 262 p.
7. Psaila S.B. Improving the practice of cyber diplomacy: trainings, tools, and other resources. 2021. URL: https://www.diplomacy.edu/wp-content/uploads/2021/10/Cyber-diplomacy-study-Diplo-Phase-I.pdf
8. Renard T. EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain // European Politics and Society. 2018. № 19 (3). P. 1-18. DOI https://doi.org/10.1080/23745118.2018.1430720
9. Riordan S. Cyber Diplomacy vs Digital Diplomacy: A Terminological Distinction. 2016. URL: https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digi-tal-diplomacy-terminological-distinction
10. Ruffini B.P. Science and Diplomacy: A New Dimension of International Relations. Springer International Publishing, 2017. 146 p.

The main threats and mechanisms to ensure the information security of the state in the field of public diplomacy

Anton V. Vlasov

Postgraduate,
Institute of Law and National Security,
Russian Presidential Academy of National Economy and Public Administration,
119571, 84, Vernadskogo ave., Moscow, Russian Federation;
e-mail: fst34@mail.ru

Abstract

The aspect of achieving information security at the national level in the field of public diplomacy is becoming increasingly important in the context of the rapid development of the Fourth Industrial Revolution, accompanied by the active development and development of the digital space. The research in this direction was carried out using analysis, synthesis, descriptive and comparative scientific methods. The article examines the approaches to achieving information security applied by states in this area from the point of view of existing threats and challenges, such as excessive freedom on the Internet and social networks, obsolescence of knowledge and competencies in the digital space, the threat of information disclosure and loss of secrecy, the culture of anonymity, hacking. In conclusion, the methods of ensuring information security in the field of public diplomacy in the Russian Federation are proposed: activation of the participation of representatives of domestic technological enterprises with the subsequent development of software and digital protection tools, as well as Internet crowdsourcing as a tool for timely delivery of verified information to a wide range of people. As effective measures to ensure information security in the field of public democracy, the development of domestic Internet sites and platforms with data storage and digital protection, as well as Internet crowdsourcing technologies, which allows providing reliable information to target users, can act.

For citation

Vlasov A.V. (2022) Osnovnye ugrozy i mekhanizmy obespecheniya informatsionnoi bezopasnosti gosudarstva v sfere publichnoi diplomatii [The main threats and mechanisms to ensure the information security of the state in the field of public diplomacy]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 11 (1A), pp. 133-139. DOI: 10.34670/AR.2022.50.22.028

Keywords

Public diplomacy, information security, digital space, threats to information security, state.

References

1. Demidov O.V. (2013) Obespechenie mezhdunarodnoi informatsionnoi bezopasnosti i rossiĭskie natsional'nye interesy [Ensuring international information security and Russian national interests]. *Indeks bezopasnosti* [Index of security], 10, 1 (104), pp. 129-168.
2. *DiploFoundation. Digital as a tool for diplomacy*. Available at: https://www.diplomacy.edu/e-diplomacy#ff1-3 [Accessed 02/02/2022]

3. Graham S. *Online Harms and the Legality Principle*. Available at: https://www.cyberleagle.com/2020/06/online-harms-and-legality-principle.html [Accessed 02/02/2022]
4. Kasper A., Vernigora V. (2021) The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market? *DEUSTO Journal of European Studies*, 65, pp. 29-71. DOI https://doi.org/10.18543/ced-65-2021pp29-71
5. Kurbalija J., Hone K. (2021) *The Emergence of Digital Foreign Policy.* Available at: https://www.diplomacy.edu/sites/default/files/2021-03/2021_The_emergence_of_digital_for- eign_policy.pdf [Accessed 02/02/2022]
6. Pamment J. (2016) *British Public Diplomacy and Soft Power: Diplomatic Influence and the Digital Revolution*. Palgrave MacMillan.
7. Psaila S.B. (2021) *Improving the practice of cyber diplomacy: trainings, tools, and other resources.* Available at: https://www.diplomacy.edu/wp-content/uploads/2021/10/Cyber-diplomacy-study-Diplo-Phase-I.pdf [Accessed 02/02/2022]
8. Renard T. (2018) EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society*, 19 (3), pp. 1-18. DOI https://doi.org/10.1080/23745118.2018.1430720
9. Riordan S. (2016) *Cyber Diplomacy vs Digital Diplomacy: A Terminological Distinction.* Available at: https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digi-tal-diplomacy-terminological-distinction [Accessed 02/02/2022]
10. Ruffini B.P. (2017) *Science and Diplomacy: A New Dimension of International Relations.* Springer International Publishing.