

Карасев Павел Александрович

кандидат политических наук, старший научный сотрудник,
Институт мировой экономики и международных отношений
имени Е. М. Примакова Российской академии наук
e-mail: karpaul@iisi.msu.ru

Pavel A. Karasev

Ph.D. (Political sciences), senior researcher,
Primakov National Research Institute of World Economy and International
relations of the Russian Academy of Sciences
e-mail: karpaul@iisi.msu.ru

ВНЕШНЯЯ ПОЛИТИКА США В КИБЕРПРОСТРАНСТВЕ ПРИ ДЖ.БАЙДЕНЕ — ПЕРВЫЕ ШАГИ

US FOREIGN POLICY IN CYBERSPACE UNDER J. BIDEN — THE FIRST STEPS

Аннотация. В современном мире проблемы информационной безопасности во всём их многообразии сильнее всего отражаются на поддержании международного мира и безопасности. Кризис отношений между США и Россией был также спровоцирован отсутствием согласованных и применяемых правил взаимодействия в ИКТ-среде. В этой связи анализ подходов к киберповестке во внешней политике новой американской администрации и прогноз их развития с точки зрения российско-американских отношений представляет собой важную и актуальную задачу.

Abstract. In the modern world, information security issues in all their diversity have a strong impact on the maintenance of international peace and security. The crisis in relations between the United States and Russia was provoked, among other things, by the lack of agreed and applicable rules for interaction in the ICT environment. In this regard, the analysis of approaches to the cyber agenda in the foreign policy of the new American administration and the

forecast of their development from the point of view of Russian-American relations is an important and urgent task.

Ключевые слова: международная информационная безопасность, кибербезопасность, кибератаки, внешняя политика США, внешняя политика России, информационное пространство.

Keywords: international information security, cyber security, cyberattacks, US foreign policy, Russian foreign policy, information space.

На саммите Россия - США 16 июня 2021 г. вопросы кибербезопасности обсуждались в приоритетном порядке, даже были приняты некоторые договоренности, в частности, о создании совместной консультативной группы. Как заявил Джо Байден по итогам саммита, одна из задач, которая поставлена перед экспертами, — выработать общее понимание того, какая критически важная инфраструктура находится за «красными линиями» [18]. К сожалению, сегодня можно лишь надеяться, что достигнутые договоренности дадут существенные результаты. Это обусловлено, прежде всего, тем, что по многим кибервопросам в американских правящих кругах наблюдается единство мнений, например, об очевидной и не требующей доказательств вине России в атаках на США. Эта позиция закреплена и в актуальных американских документах стратегического планирования, где Россия и Китай, наряду с Северной Кореей и Ираном, определены как главные источники киберугроз [15, P.2]. Также большую роль играет инерция административно-управленческого аппарата. Байден опирается на результаты работы своего предшественника. Все эти факторы значительно ограничивают пространство для политических маневров в киберсфере.

Наследие

Дональд Трамп предпринял несколько действий, которые сегодня определяют внешнюю политику США в киберсфере. Во-первых, был повышен статус Киберкомандования, оно получило новые полномочия [8].

Кроме защиты информационных сетей Министерства обороны, эта структура осуществляет все виды военных киберопераций [9, P.1]. Были приняты концепции «постоянного противодействия» (persistent engagement) и «обороны за передовой линией» (defend forward) [14]. Их реализация предполагает непрерывное проведение тайных киберопераций в сетях потенциальных противников, в том числе для оказания превентивного воздействия. До выборов Байден неоднократно повторял [6], что заставит Россию «поплатиться» за злонамеренное поведение в киберпространстве, в том числе за приписываемое ей вмешательство в американские выборы. Одновременно он высказывался в пользу более взвешенной политики, сообщив, что стратегия «постоянного противодействия» будет пересмотрена [7].

При Трампе была принята Национальная киберстратегия США 2018 г., где выделено четыре направления: защита американских граждан, страны и американского образа жизни; содействие процветанию Америки; поддержание мира силой; распространение американского влияния [15, P.3]. В рамках «поддержания мира силой» была представлена «инициатива киберсдерживания», направленная на привлечение к ответственности государств, совершающих злонамеренные действия в киберпространстве. Вместо должного расследования и разбирательства, используется т. н. «публичная атрибуция», в рамках которой виновный «назначается» из политических соображений. После этого можно применять все доступные меры — от экономических санкций до кибератак. Перед выборами Джо Байден обещал «приложить усилия по установлению всеобъемлющих кибернорм» [7]. Он фактически заявил, что политика Д. Трампа будет продолжена.

Нельзя исключать и того, что в полной мере будет реализовываться стратегия «многоуровневого киберсдерживания», представленная в докладе Комиссии соляриума по вопросам киберпространства (The Cyberspace Solarium Commission) [12], созданной в 2019 г., в соответствии с положением

Закона 2019 г. о бюджетных ассигнованиях на национальную оборону [13, Sec. 1652]. Под множеством уровней предполагается использование всех доступных инструментов — от дипломатических до военных.

Первые шаги

Несмотря на то, что администрация Байдена ещё не опубликовала значимых стратегических документов по вопросам кибербезопасности, уже можно сделать выводы о содержании и направленности её политики в этой сфере. В апреле 2021 г. пресс-служба Белого дома опубликовала информационный бюллетень о «противодействии осуществляемой Россией вредоносной деятельности за рубежом» [11]. Этот документ, помимо санкций и иных мер, содержит раздел о глобальном подходе к кибербезопасности.

Прежде всего, Соединенные Штаты активизируют усилия по продвижению ответственного поведения государств в киберпространстве и сотрудничеству с союзниками и партнерами для противодействия злонамеренной деятельности в киберпространстве. Как уже было сказано, Джо Байден на практике продолжает политику Трампа.

Вторым пунктом программы объявлено о создании в 2021 г. первого в своем роде курса для политиков всего мира по политическим и техническим аспектам публичной атрибуции киберинцидентов. Также будет проходить обучение юристов-международников и политиков возможностям применения международного права к поведению государства в киберпространстве. Как сказал Сергей Лавров в ходе пресс-конференции по итогам 2020 г., за пределами ООН создаются «эксклюзивные механизмы, группы так называемых единомышленников», решения которых пытаются навязать всем участникам международных отношений [2]. Публичная атрибуция — это яркий пример подобного механизма. В феврале 2021 г. Джейк Салливан, советник президента США по национальной безопасности, обещал, что ответ администрации Байдена на приписываемый России взлом SolarWinds «будет включать сочетание видимых и невидимых инструментов» [16]. Можно утверждать, что организация курсов по атрибуции — это чёткий сигнал о

намерениях двигаться в сторону конфронтации, а не сотрудничества. Они будут реализованы на базе Центра европейских исследований в области безопасности им. Дж. Маршалла в Гармиш-Партенкирхене. В этом городе в Германии на протяжении более 10 лет проводились международные научные форумы «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», организатором которых был МГУ имени М.В. Ломоносова при поддержке аппарата Совета Безопасности Российской Федерации и Министерства иностранных дел Российской Федерации. Это мероприятие позволило ученым, экспертам, представителям государственных структур и бизнес-сообщества различных стран открыто и в дружественной обстановке обсуждать наиболее острые проблемы и вызовы международной информационной безопасности, а также вырабатывать взаимоприемлемые решения.

Третьим шагом является сохранение приверженности коллективной безопасности в киберпространстве. Министерство обороны США привлекает союзников к учениям Cyber Flag 21-1. На официальном уровне заявлено, что эти учения призваны повысить оборонительные возможности в киберпространстве и устойчивость к кибератакам. Подобное усиление «киберфронта» едва ли укладывается в идею пересмотра концепции постоянного противодействия и обороны за передовой линией в сторону смягчения, о чём сообщалось до выборов.

Перспективы

В мае 2021 г. произошла кибератака на трубопровод Colonial Pipeline. Реакция американской стороны была сдержанной. Президент Байден отметил, что «нет доказательств того, что Россия принимала в этом участие» [10]. Кроме того, он подчеркнул, что: «Мы работаем над тем, чтобы создать некий международный стандарт, согласно которому, когда правительства знают, что с их территории осуществляется преступная деятельность, мы совместно противодействуем этим преступным группам. Я полагаю, что это

станет одним из вопросов, о которых я буду говорить с президентом Путиным» [20].

Предложение к США перезагрузить отношения в сфере использования информационно-коммуникационных технологий (ИКТ) и возобновить диалог по вопросам международной информационной безопасности поступило от России осенью 2020 г. [1], а начало диалогу было положено ещё в 2013 г. с принятием Совместного заявления о новой области сотрудничества в укреплении доверия [3]. После обострения двусторонних отношений в 2016 г. совместная деятельность была заморожена.

В ходе саммита была достигнута договоренность начать диалог в формате консультаций — это важный шаг к восстановлению доверия. Однако практическая реализация возможных договоренностей осложнена политическими факторами. Существует запрет для органов Федерального правительства США, кроме Министерства обороны, на заключение с Россией двустороннего соглашения или создание совместной группы или подразделения по кибербезопасности [19, Sec. 6701]. Для того чтобы подобное соглашение или группа были созданы, директор Национальной разведки США должен представить в профильные комитеты Конгресса соответствующий доклад с указанием ожидаемой пользы для национальной безопасности. Вероятность позитивной оценки представляется низкой. Согласно «Ежегодной оценке угроз разведывательного сообщества США 2021 г.», «Россия остается главной киберугрозой, поскольку она совершенствует и использует свои возможности в сфере кибершпионажа, оказания влияния и кибератак» [5, P.10].

Диалог между США и Россией необходим, и Джо Байден, как представляется, это понимает. Надежда на позитивный результат подкрепляется тем, что, развивая договоренности, достигнутые в Женеве, лидеры двух стран подчеркнули «необходимость предметного и конструктивного сотрудничества в области кибербезопасности, продолжения

соответствующих контактов» [4]. По имеющимся сообщениям, встреча совместной российско-американской комиссии по кибербезопасности состоится в июле 2021 г. [17]

Как было сказано выше, есть существенные препятствия для заключения российско-американского соглашения по кибербезопасности. При этом нет никаких ограничений для сотрудничества в многостороннем формате. В годы президентства Б. Обамы вопросам международного сотрудничества в ИКТ-среде придавалось большое значение. Наряду с Россией, США активно участвовали в работе Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, в результате которой в 2015 г. были приняты нормы, принципы и правила ответственного поведения государства в ИКТ-среде. Есть надежда, что при Джо Байдене конструктивная работа на этой площадке будет восстановлена и удастся решить вопросы, связанные с применением указанных норм, принципов и правил ответственного поведения на практике. Другим возможным направлением может стать договоренность, которая позволит снизить киберриски в наиболее чувствительных для национальной безопасности сферах – критически важной гражданской и военной инфраструктуре, включая информационно-управляющие системы ядерных сил и ПРО.

Список источников и литературы:

1. Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности, 25.09.2020 // Президент России: официальный сайт. - URL: <http://www.kremlin.ru/events/president/news/64086>.
2. Лавров: РФ обеспокоена действиями США и союзников по подрыву международной безопасности, 18.01.2021 // ТАСС: [Интернет-ресурс]. - URL: <https://tass.ru/politika/10482819>.

3. Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия, 17.06.2013 // Президент России: (официальный сайт). - URL: <http://www.kremlin.ru/supplement/1479>.
4. Телефонный разговор с Президентом США Джоозефом Байденом, 09.07.2021 // Президент России: (официальный сайт). - URL: <http://kremlin.ru/events/president/news/66172>.
5. 2021 Annual Threat Assessment of the U.S. Intelligence Community // Office of the Director of National Intelligence [Official website] - URL: <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf>.
6. Campaign 2020: Trump-Biden Second Debate // C-Span [Web-source]. - URL: <https://www.c-span.org/video/?475796-1/trump-biden-debate&live>.
7. Cyber Policy // The New York Times [Web-source]. - URL: <https://www.nytimes.com/interactive/2020/us/politics/2020-democrats-cyber-policy-foreign-policy.html>.
8. David E. Sanger, Trump Loosens Secretive Restraints on Ordering Cyberattacks, 20.09.2018 // The New York Times [Web-source]. - URL: <https://www.nytimes.com/2018/09/20/us/politics/trump-cyberattacks-orders.html>.
9. Defense Primer: Cyberspace Operations // Federation of American Scientists [Official website]. - URL: <https://fas.org/sgp/crs/natsec/IF10537.pdf>.
10. Dustin Volz, U.S. Blames Criminal Group in Colonial Pipeline Hack, 10.05.2021 // The Wall Street Journal [Web-source]. - URL: <https://www.wsj.com/articles/fbi-suspects-criminal-group-with-ties-to-eastern-europe-in-pipeline-hack-11620664720>.
11. FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government // The White House [Official website]. - URL: <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government>.

12. Final Report // The Cyberspace Solarium Commission [Official website]. - URL: https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.
13. H.R.5515 – John S. McCain National Defense Authorization Act for Fiscal Year 2019 // Congress.gov [Official website]. - URL: <https://www.congress.gov/bill/115th-congress/house-bill/5515/text>.
14. Mark Pomerleau, Defense officials taking advantage of new cyber authorities, 27.11.2018 // Fifth Domain [Web-source]. - URL: <https://www.fifthdomain.com/dod/cybercom/2018/11/27/defense-officials-taking-advantage-of-new-cyber-authorities/>
15. National Cyber Strategy of the United States of America // The White House (archive) [Official website]. - URL: <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.
16. Oleg Brunov, US Vows 'Mix of Tools Seen and Unseen' Against Russia for Its Alleged Involvement in SolarWinds Hack, 22.02.2021 // Sputnik News [Web-source]. - URL: <https://sputniknews.com/us/202102221082147818-us-vows-mix-of-tools-seen-and-unseen-against-russia-for-its-alleged-involvement-in-solarwinds-hack>.
17. Remarks by President Biden Before Air Force One Departure, July 9, 2021 // The White House [Official website]. - URL: <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/09/remarks-by-president-biden-before-air-force-one-departure-5>.
18. Remarks by President Biden in Press Conference, June 16, 2021 // The White House [Official website]. - URL: <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/06/16/remarks-by-president-biden-in-press-conference-4/>
19. S.1790 – National Defense Authorization Act for Fiscal Year 2020 // Congress.gov [Official website]. - URL: <https://www.congress.gov/bill/116th-congress/senate-bill/1790/text>.

20. Tonya Riley, The Cybersecurity 202: Biden says the Russian government was not involved with Colonial Pipeline hack, 14.05.2021 // The Washington Post [Web-source]. - URL: <https://www.washingtonpost.com/politics/2021/05/14/cybersecurity-202-biden-says-russian-government-was-not-involved-with-colonial-pipeline-hack/>