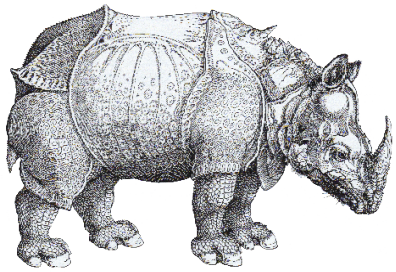


ИНДЕКС БЕЗОПАСНОСТИ №8 (22) | 2021

НАУЧНЫЕ ЗАПИСКИ

Сергей Себекин

Новая киберэпоха: как США вступают в глобальную конкуренцию в киберпространстве

ПИРПРЕСС

МОСКВА, 2021

Главный редактор: В.А. Орлов

Редактор: Н.С. Дегтярёв

Рецензент: В.Б. Козюлин

Себекин Сергей Александрович. Новая киберэпоха: как США вступают в глобальную конкуренцию в киберпространстве / Ред. Н.С. Дегтярёв. М.: ПИР-Пресс, 2021. – 46 с. – (*Индекс Безопасности* – Научные записки).

Данная научная записка посвящена новой стратегии кибербезопасности США, которая перешла от традиционной политики сдерживания к политике постоянной вовлечённости. Автор обращает внимание на её критику экспертным сообществом ввиду того, что она может привести к милитаризации киберпространства, а также даёт рекомендации, полезные России при взаимодействии с США по вопросам кибербезопасности.

Данная научная записка и другие материалы научной серии размещены на сайте: http://pircenter.org/articles

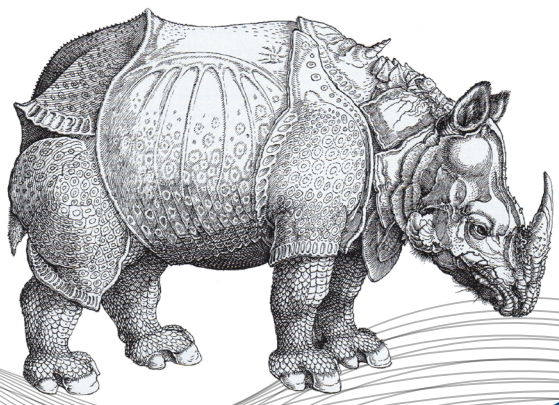
АВТОР

СЕБЕКИН, Сергей

Кандидат исторических наук (тема кандидатской диссертации: «Генезис и развитие стратегий сдерживания киберугроз в США, КНР и России (1990-е–2014 гг.)»), преподаватель кафедры политологии, истории и регионоведения Иркутского государственного университета.

Стипендиат Оксфордского Российского фонда 2014-2015 гг. В 2016 г. проходил стажировку в университете Хоккайдо в рамках Российско-Японской программы Russia-Japan East 3 (RJE 3), г. Саппоро, Япония. В 2020-2021 гг. проходил стажировку в ПИР-Центре по программе «Новые технологии и международная безопасность». Участник XX Международной Школы ПИР-Центра по проблемам глобальной безопасности. Автор публикаций по проблематике международной кибербезопасности. Участник всероссийских и международных форумов и конференций.

Сфера научных интересов: гуманитарные проблемы кибербезопасности, национальные концепции и стратегии кибербезопасности, теории кибервойны, доктрина киберсдерживания, применимость международного права к кибер конфликтам, международные процессы в сфере международной кибербезопасности.



Оглавление

Главное

- **В последнее время в военно-стратегической и экспертной мысли США всё чаще можно слышать заявления о том, что мир вступает в долгосрочную стратегическую конкуренцию великих держав.**

- **Согласно экспертной и стратегической мысли США, устоявшаяся стратегия сдерживания киберугроз, базирующаяся только на двух методах – наказания и воспрещения – неэффективна. Поэтому существующая концепция кибербезопасности нуждается в модернизации и переходе к стратегии постоянной вовлечённости.**

- **Происходящие концептуальные изменения сопровождаются реальной эволюцией военно-политических институтов и изменением соответствующей политики с той целью, чтобы новая стратегия постоянной вовлечённости могла быть реализована на практике.**

- **В ходе постоянной вовлечённости посредством негласных переговоров Соединённые Штаты рассчитывают прояснить различие между приемлемым/неприемлемым поведением в киберпространстве и стимулировать процесс формирования правил приемлемого поведения в киберпространстве за счёт постепенного накопления эмпирического опыта другими странами.**

- **В новых стратегических документах США не делается адекватных попыток изучить возможную эскалацию, которая может возникнуть вследствие применения стратегии постоянной вовлечённости**

- **США не готовы дожидаться какой-либо позитивной динамики в переговорах по вопросу обеспечения международной кибербезопасности, уже сейчас явно превращают киберпространство в место проведения активных операций и милитаризируют его.**

Новая киберэпоха: как США вступают в глобальную конкуренцию в киберпространстве

Сергей Себекин

ВВЕДЕНИЕ[1]

Сегодня Россия и Соединённые Штаты переживают не самый лучший период в своих взаимоотношениях. И к сожалению, киберповестка стала одним из наиболее отягчающих факторов в этих взаимоотношениях. В этом плане именно период президентства Дональда Трампа, пожалуй, стал одним из наиболее напряжённых для взаимодействия Москвы и Вашингтона по вопросу киберповестки. После выборов президента США в 2016 г. в сторону России стали систематически поступать обвинения во вмешательстве в американский демократический процесс и кибератаках на системы Соединённых Штатов. И хотя сам Дональд Трамп полностью отрицал какую-либо помощь якобы со стороны российских спецслужб и старался игнорировать проблему предполагаемого российского вмешательства, именно в период его президентства произошли ключевые военно-политические изменения в стратегии обеспечения кибербезопасности США.

От более оборонительной и «пассивной» стратегии Барака Обамы, основанной на сдерживании киберугроз, военно-политическое руководство Дональда Трампа перешло к более проактивной и конфронтационной стратегии – стратегии постоянной вовлечённости.

Более того, в Вашингтоне пришли к выводу, что сегодня в киберпространстве получает своё распространение стратегическая конкуренция великих держав, для участия в которой и нужна новая стратегия постоянной вовлечённости.

Итак, в данной работе будет рассмотрено, какие ключевые военно-политические изменения произошли в сфере обеспечения кибербезопасности в США в последние годы, как концептуально изменился «ландшафт» киберпространства, как США вступают в стратегическую конкуренцию и принимают новую стратегию постоянной вовлечённости, и какие политико-институциональные изменения произошли в связи с принятием нового стратегического подхода.

Можно сказать, что в данной работе будет сделана попытка,

[1] Автор и редактор данного номера благодарят за ценные замечания и комментарии Вадима Козюлина, Владимира Орлова, Илону Стадник, Дмитрия Стефановича, Анастасию Толстухину, Александра Федорова, Олега Шакирова и Михаила Якушева.

во-первых, подвести некие «киберитоги» президентства Дональда Трампа, и, во-вторых, предположить, что с оставленным ему «кибернаследством» будет делать новый глава Белого дома Джо Байден.

Актуальность работы обусловлена самой сложившейся между Соединёнными Штатами и Россией на сегодняшний день стратегической ситуацией, в том числе и по вопросу киберповестки. Надо отметить, что по заявлениям американских СМИ, кибербезопасность станет одним из главных приоритетов новой администрации Джо Байдена[2]. Соответственно, понимание подходов Соединённых Штатов к обеспечению национальной кибербезопасности и ключевых стратегических изменений в них крайне важно как для формирования российской стратегии кибербезопасности, так и для разработки дальнейшей политики по взаимодействию с Вашингтоном в рамках киберповестки.

Для целей данного доклада необходимо иметь в виду различия в понятийно-терминологической базе в области обеспечения безопасности кибернетических информационных систем России и Соединённых Штатов.

Так, в США употребляется термин «кибер-», под которым понимаются технологические аспекты, связанные с цифровыми технологиями – сетями, компьютерами, системами и т.д. (сюда же относятся и «технологические» операции с информацией). В России же используют термин «информационный», в значение которого вкладываются как информационно-психологические аспекты (в т.ч. и манипуляции с информацией), так и технологические аспекты. В России термин «кибер-» встречает сильное сопротивление, а в официальных документах вообще отсутствует.

Важно, что в отечественном дискурсе технологические аспекты безопасности является частью стратегически более широкой информационной безопасности, в США же наоборот – информационная безопасность выступает частью стратегии кибербезопасности. Поскольку в центре внимания данного доклада американская стратегия, то с целью соблюсти адекватное и эквивалентное понимание американского дискурса здесь будет употребляться термин «кибер-» в том смысле, в каком он понимается в США.

Итак, *кибербезопасность* – набор средств, методов, стратегий, принципов, процессов и технологий, предназначенных для защиты вычислительных устройств (компьютеров, смартфонов, планшетов), компьютерных систем, сетей и сайтов, а также любого оборудования или объекта, связанного с ними или управляемого ими, подключенных к глобальной или локальной сети, от кибератак и любого несанкционированного доступа, использующих уязвимости в установленном программном обеспечении и влекущих их повреждения, отключение, выход из строя, кражу хранящейся на них информации и иные пагубные последствия.

[2] Solender A. 'I Will Not Stand Idly By': Biden Says Cybersecurity Will Be 'Top Priority' After Giant Hack [Electronic resource] / Forbes. Washington, DC, 2020. Mode of access: https://www.forbes.com/sites/andrewsolender/2020/12/17/i-will-not-stand-idly-by-biden-says-cybersecurity-will-be-top-priority-after-giant-hack/?sh=1caf38245159 (date of access: 24.02.2021); Perry T. Kamala Harris plans to prioritize cybersecurity and global health in foreign policy platform [Electronic resource] / CBS News. Washington, DC, 2021. Mode of access: https://www.cbsnews.com/news/kamala-harris-plans-to-prioritize-cybersecurity-and-global-health-in-foreign-policy-platform/ (date of access: 24.02.2021).

«СТАРАЯ» СТРАТЕГИЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ – СТРАТЕГИЯ КИБЕРСДЕРЖИВАНИЯ

Взятая на вооружение при Джордже Буше Мл. стратегия сдерживания киберугроз получила своё активное развитие при Бараке Обаме и была краеугольным камнем в обеспечении кибербезопасности США в период его президентства.

Как известно, сдерживание своими корнями уходит в эпоху Холодной войны. Первоначально сдерживание было направлено против применения ядерного оружия и отчасти основывалась на взаимно-гарантированном уничтожении[3]. С наступлением цифровой эпохи и возникновением нового типа угроз – киберугроз – эксперты и политики США «по инерции» стали размышлять над тем, как применить стратегию сдерживания к кибератакам. Таким образом, американская военно-политическая и экспертная мысль при формировании стратегии киберсдерживания взяла за основу модель ядерного (и иногда неядерного – конвенционального) сдерживания, экстраполируя её ключевые принципы на киберпространство[4].

Исходя из этого, основные обсуждения стратегии киберсдерживания стали строится вокруг двух методов, характерных для «классической» стратегии сдерживания:

1) Путём наказания (от англ. – «deterrence by punishment»), заключающемся в проведении соразмерных ответных мер, которые могут включать в себя как пропорциональные по масштабу и последствиям кибератаки, так и военный ответ с использованием традиционных вооружённых сил (в теории). Более того, сдерживание путём наказания предполагает использование всех возможных инструментов национальной власти – дипломатических, экономических, правовых и т.д.

2) Путём воспрещения (от англ. – «deterrence by denial»), достигаемого посредством улучшения обороны. Сдерживание воспрещением заключается в том, чтобы минимизировать получаемые агрессором выгоды, или сделать так, чтобы затраты не оправдали ожидаемых результатов, и тем самым убедить его в бессмысленности осуществления кибератак[5].

---

[3] Kennan G. F. «The Sources of Soviet Conduct» [Electronic resource] / Foreign Affairs. New York, NY, 1947. Mode of access: https://www.foreignaffairs.com/articles/russian-federation/1947-07-01/sources-soviet-conduct (date of access: 18.07.2020); Kennan G. F. Russia, The Atom and the West. New York : Harper & Brothers, 1958. P. 120; Rothschild E. What Is Security? [Electronic resource] / Daedalus. 1995. Vol. 124, No. 3. P. 58. Mode of access: https://www.jstor.org/stable/20027310?read-now=1&refreqid=excelsior%3A46a6a56cbec5604acaac4e7644662a66&seq=1#page_scan_tab_contents (date of access: 18.07.2020)

[4] Healey J. Not The Cyber Deterrence the United States Wants [Electronic resource] / Council on Foreign Rela-tions. New York, NY, 2018. Mode of access: https://www.cfr.org/blog/not-cyber-deterrence-united-states-wants (date of access: 18.07.2020); Fischerkeller M. P., Harknett R. J. Persistent Engagement and Tacit Bar-gaining: A Path Toward Constructing Norms in Cyberspace [Electronic resource] / Lawfare. Washington, DC, 2018. Mode of access: https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace (date of access: 18.07.2020); Sulmeyer M. How the U.S. Can Play Cyber-Offense: Deterrence Isn't Enough [Electronic resource] / Foreign Affairs. New York, NY, 2018. Mode of access: https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense (date of access: 18.07.2020).

[5] Jasper S. Strategic Cyber Deterrence: The Active Cyber Defense Option. New York : Row-man & Littlefield, 2017. P. 15, 111.

Вопрос о классических методах сдерживания – путём наказания или путём воспрещения – стал центральным в обсуждении стратегии киберсдерживания в США[6].

Так или иначе, но в военно-политической мысли Соединённых Штатов киберсдерживание «балансирует» именно между этими двумя методами, вокруг которых развернулись основные обсуждения стратегии. Согласно «Международной стратегии по действиям в киберпространстве» от 2011 г., США будут «стремиться сдерживать тех, кто угрожает миру и стабильности посредством действий в киберпространстве. [против США. – С.А.] делать это с помощью совпадающих политик, которые сочетают *устойчивость национальных и международных сетей* с активным мониторингом и *целым рядом надежных вариантов реагирования*»[7].

Стратегия киберсдерживания отражена во многих важнейших стратегических документах США. Так, например, в «Киберстратегии Министерства обороны США» от 15 апреля 2015 г. было сказано, что «Соединённые Штаты будут и впредь *реагировать на кибератаки [...] любым способом и в любом месте по нашему выбору, используя соответствующие инструменты власти США* ...]»[8]. Отметим, что ключевое слово здесь – реагировать – подразу-

[6] Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency [Electronic resource] / Center for Strategic and International Studies. Washington, DC, 2008. P. 26. Mode of access: http://cs.brown.edu/courses/csci1950-p/sources/2008_CSIS_SecuringCyberspace_44.pdf (date of access: 21.07.2020); Nye J. S. Deterrence and Dissuasion in Cyberspace [Electronic resource] / Inter-national Security. Winter 2016/2017. Vol. 41, No 3. P. 54, 58. Mode of access: https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266 (date of access: 21.07.2020); Denning D. Cybersecurity's Next Phase: Cyber-deterrence [Electronic resource] / The Conversation. Waltham, MA, 2016. Mode of access: https://theconversation.com/cybersecuritys-next-phase-cyber-deterrence-67090 (date of access: 21.07.2020); Geers K. The Challenge of Cyber Attack Deterrence [Electronic resource] / Computer Law & Security Review. 2010. No. 26. P. 299, 302. Mode of access: https://www.sciencedirect.com/science/article/abs/pii/S0267364910000506 (date of access: 21.07.2020); Goodman W. Cyber Deterrence: Tougher in Theory than in Practice? [Electronic resource] / Strategic Studies Quarterly. 2010. Vol. 4, No. 3. P. 108. Mode of access: https://www.jstor.org/stable/26269789?seq=1#metadata_info_tab_contents (date of access: 21.07.2020); Li-bicki M. C. Cyberdeterrence and Cyberwar [Electronic resource] / RAND Corporation. Santa Monica, CA, 2009. P. 7, 8. Mode of access: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (date of access: 22.07.2020); Meakins J. Living in (Digital) Denial Russia's Approach to Cyber Deterrence: Euro-Atlantic Se-curity Report [Electronic resource] / European Leadership Network. 2018. P. 4. Mode of access: https://www.europeanleadershipnetwork.org/wp-content/uploads/2018/07/Living-in-Digital-Denial-Russia%E2%80%99s-Approach-to-Cyber-Deterrence.pdf (date of access: 22.07.2020); Snyder G. H. Deterrence and Defense: Toward a Theory of National Security. Princeton, NJ : Princeton University Press, 1961. P. 14-16; Jasper S. Strategic Cyber Deterrence... P. 85-136; Arquilla J. Deterrence After Stuxnet [Electronic resource] / Commmunications of the ACM. New York, NY, 2015. Mode of access: https://cacm.acm.org/blogs/blog-cacm/190371-deterrence-after-stuxnet/fulltext (date of access: 22.07.2020); Lynn W. J. Defending a New Domain: The Pentagon's Cyberstrategy [Electronic resource] / Foreign Affairs. Vol. 89, No 5. P. 99-100. Mode of access: https://www.jstor.org/stable/20788647?read-now=1&seq=3#page_scan_tab_contents (date of access: 22.07.2020).

[7] International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World [Electronic resource] / The White House. Washington, DC, 2011. P. 12. Mode of access: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (date of access: 23.07.2020).

[8] The Department Of Defense Cyber Strategy [Electronic resource] / U.S. Department Of Defense. Washington, DC, 2015. P. 10. Mode of access: (date of access: 23.07.2020). http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf (date of access: 23.07.2020).

мевает собой принятие определённых мер уже *постфактум*.

Помимо «Киберстратегии Министерства обороны» и «Международной стратегии по действиям в киберпространстве», приверженность стратегии киберсдерживания с балансом в сторону того или иного метода была подтверждена в таких официальных документах, как «Доклад Министерства обороны США по вопросам политики киберпространства» от 2011 г.[9], «Отчёт целевой группы по киберсдерживанию» от 2017 г.[10] и т.д. Однако первым *официальным* документом, установившим сдерживание кибератак как явную цель последующих усилий правительства США, стала «*Национальная стратегия по защите киберпространства*» от 2003 г.

Необходимо также отметить, что важным условием для эффективного осуществления киберсдерживания является наличие *порогов допустимого ущерба, превышение которых повлечёт за собой осуществление определённых пропорциональных ответных мер разного уровня*[11]. То есть, «классическое» *киберсдерживание подходит только для тех кибератак, которые достигают или превышают установленный порог допустимого ущерба, после которого кибератака начинает квалифицироваться как акт агрессии.*

Однако, согласно современной американской стратегической мысли, «традиционное» киберсдерживание путём наказания и воспрещения оказалось неэффективным в условиях так называемой *долгосрочной стратегической конкуренции великих держав.*

Традиционное американское киберсдерживание оказалась неэффективным в условиях долгосрочной стратегической конкуренции великих держав

СТРАТЕГИЧЕСКАЯ КОНКУРЕНЦИЯ ВЕЛИКИХ ДЕРЖАВ

В последнее время в военно-стратегической и экспертной мысли США всё чаще можно слышать заявления о том, что мир вступает в *долгосрочную стратегическую конкуренцию великих держав*[12]. Но что такое стратегическая конкуренция?

---

[9] Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 [Electronic resource] / U.S. Department Of Defense. Washington, DC, 2011. P. 2, 5. Mode of access: https://fas.org/irp/eprint/dod-cyber.pdf (date of access: 23.07.2020).

[10] Task Force on Cyber Deterrence [Electronic resource] / Office of the Under Secretary of Defense for Acquisi-tion, Technology, and Logistics. Washington, DC, 2017. P. 6. Mode of access: https://www.hsdl.org/?abstract&did=799190 (date of access: 23.07.2020).

[11] Libicki M. C. Cyberdeterrence and Cyberwar. P. 17, 65, 102; Libicki M. C. It Takes More than Offensive Ca-pability to Have an Effective Cyberdeterrence Posture: Testimony presented before the House Armed Ser-vices Committee [Electronic resource] / RAND Corporation. Santa Monica, CA, 2017. P. 1, 4, 5, 7. Mode of access: https://www.rand.org/pubs/testimonies/CT465.html (date of access: 23.07.2020); Goodman W. Cyber Deterrence... P. 127-129; Geers K. The Challenge of Cyber... P. 302; Jasper S. Strategic Cyber Deterrence... P. 231; Meakins J. Living in (Digital) Denial Russia's Approach to Cyber Deterrence. P. 13; Pomerleau M. Cyber Red Lines: Ambiguous by Necessity? [Electronic resource] / C4ISRNET. Tysons, Virginia, 2016. Mode of ac-cess: https://www.c4isrnet.com/2016/09/09/cyber-red-lines-ambiguous-by-necessity/ (date of access: 25.07.2020).

[12] Mazarr M. J. [et al.] Understanding the Emerging Era of International Competition: Theoretical and Historical Perspectives [Electronic resource] / Rand Corporation. Santa Monica, CA, 2018. 47 p. Mode of access: (date of access: 25.07.2020); Burkhart D., Woody A. Strategic Competition: Beyond Peace and War [Electronic resource] / Joint Force Quarterly. 2017. Vol. 86. 3rd Quarter. P. 20-27. Mode of access: https://ndupress.ndu.edu/Publications/Article/1219140/strategic-competition-beyond-peace-and-war/ (date of access: 25.07.2020); Haffa R. P. The Future of Conventional Deterrence: Strategies for Great Power Com-petition [Electronic resource] / Strategic Studies Quarterly. 2018. Vol. 12, No. 4. P. 94-115. Mode of access: https://www.jstor.org/stable/26533617?seq=1#metadata_info_tab_contents (date of access: 25.07.2020). https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2726/RAND_RR2726.pdf (date of access: 25.07.2020); Burkhart D., Woody A. Strategic Competition: Beyond Peace and War [Electronic resource] / Joint Force Quarterly. 2017. Vol. 86. 3rd Quarter. P. 20-27. Mode of access: https://ndupress.ndu.edu/Publications/

Стратегическая конкуренция великих держав (от англ. – «*great-power competition*») – такое состояние международных отношений и глобальной стратегической ситуации, при котором государства (соответственно – мировые державы) стремятся максимизировать свои военные, политические и экономические интересы, и минимизировать эти интересы у соперника в международной системе.

Впервые о том, что мир вступает в эпоху стратегической конкуренции, было заявлено в «Стратегии национальной безопасности США» от декабря 2017 г. В ней говорилось, что, будучи феноменом XX в., «конкуренция великих держав вернулась»[13].

Более полно тезис о вступлении Соединённых Штатов в эпоху стратегической конкуренции был раскрыт в «Стратегии национальной обороны США» от января 2018 г. Согласно стратегии, сегодня глобальная среда характеризуется «*возрождением долгосрочной стратегической конкуренции между странами*»[14]. Именно возрождение межгосударственной долгосрочной стратегической конкуренции, а не терроризм, сегодня является главным вызовом безопасности для Соединённых Штатов[15]. В этих условиях противники США наращивают усилия по осуществлению тех враждебных действий, которые *не достигают уровня вооружённого конфликта*[16]. В связи с этим, США также будут «расширять конкурентное пространство» для сохранения стратегической инициативы[17].

Однако, в «Стратегии национальной безопасности США» и в «Стратегии национальной обороны США» о том, что Соединённые Штаты вступают в долгосрочную стратегическую конкуренцию говорится в общем стратегическом контексте, а не в контексте киберпространства.

КАК КИБЕРПРОСТРАНСТВО СТАЛО ПРОСТРАНСТВОМ ПОСТОЯННОЙ СТРАТЕГИЧЕСКОЙ КОНКУРЕНЦИИ?

Совершенно очевидно, что в стратегической мысли Соединённых Штатов киберпространство стало рассматриваться пространством, в котором точно так же получает своё распространение долгосрочная стратегическая конкуренция. Однако, почему киберпространство вдруг стало пространством стратегической конкуренции?

Дело в том, что в последнее время развернулись активные обсуждения уникальной природы киберпространства, выя-

Article/1219140/strategic-competition-beyond-peace-and-war/ (date of access: 25.07.2020); Haffa R. P. The Future of Conventional Deterrence: Strategies for Great Power Com-petition [Electronic resource] / Strategic Studies Quarterly. 2018. Vol. 12, No. 4. P. 94-115. Mode of access: https://www.jstor.org/stable/26533617?seq=1#metadata_info_tab_contents (date of access: 25.07.2020).

[13] National Security Strategy of the United States of America [Electronic resource] / The White House. Washing-ton, DC, 2017. P. 27. Mode of access: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (date of access: 26.07.2020).

[14] Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge [Electronic resource] / Department of Defense. Washington, DC, 2018. P. 2. Mode of access: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (date of access: 26.07.2020).

[15] Summary of the 2018 National Defense Strategy of the United States of America... P. 1, 2.

[16] Summary of the 2018 National Defense Strategy of the United States of America... P. 2, 3.

[17] Summary of the 2018 National Defense Strategy of the United States of America... P. 4, 5.

вив его концептуальные отличия от традиционных операционных сред – суши, моря и воздуха – что вполне закономерно.

Самые главное отличие, которое важно выделить для целей данного исследования – это *взаимосвязанность* киберпространства[18]. В отличие от «физических» суши, моря, и воздуха, которые «сегментированы» и над которыми государства осуществляют свой суверенитет в рамках национальных границ, киберпространство таковых границ не имеет, и поэтому оно *взаимосвязано*[19]. Например, экс-заместитель министра обороны Патрик Шэнахэн[20] заявил, что «киберпространство принципиально отличается от других областей боевых действий, поскольку оно не связано физическими ограничениями»[21].

Экс-заместитель министра обороны Патрик Шэнахэн во время сессии вопросов и ответов в Пентагоне (Вашингтон, 2018 г.)

Источник: www.fifthdomain.com

Вместе с этим существуют и другие важные особенности киберпространства, которые влияют на характер взаимодействия государств между странами в нём. Во-первых, киберпространство создано не природой, а является искусственной конструкцией, из-за чего оно имеет «способность» к технологической эволюции и модернизации. То есть, в отличие от традиционных пространств, которые могут *лишь изменяться* под воздействием человеческой деятельности, киберпространство продолжает формироваться совершенно различными субъектами – как государствами, так и негосударственными игроками. Во-вторых, вопросы суверенитета очень неоднозначны в киберпространстве, и в настоящее время нет международно-согласованной концепции суверенитета в киберпространстве[22]. Это значит, что государства и другие субъекты международных отношений будут постоянно стремится оказывать свое влияние в киберпространстве посредством кибероперций.

[18] Fischerkeller M. P., Harknett R. J. Deterrence is Not a Credible Strategy for Cyberspace [Electronic resource] / Orbis. 2017. Vol. 61, Issue 3. P. 391. Mode of access: https://www.sciencedirect.com/science/article/abs/pii/S0030438717300431 (date of access: 29.07.2020); Fischerkeller M. P., Harknett R. J. What Is Agreed Competition in Cyberspace? [Electronic resource] / Law-fareWashington, DC, 2019. Mode of access: https://www.lawfareblog.com/what-agreed-competition-cyberspace (date of access: 29.07.2020); Harknett R. J. Progress Is the Promise in National Cybersecurity Strategy [Electronic resource] / Lawfare. Washington, DC, 2020. Mode of access: https://www.lawfareblog.com/progress-promise-national-cybersecurity-strategy (date of access: 29.07.2020); Goldman E. O. From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy [Electronic resource] / Texas National Security Review. Special Issue: Cyber Competition. 2020. Vol. 4, Issue 3. Mode of access: https://tnsr.org/2020/09/from-reaction-to-action-adopting-a-competitive-posture-in-cyber-diplomacy/ (date of access: 20.10.2020).

[19] Fischerkeller M. P., Harknett R. J. What Is Agreed Competition in Cyberspace?
Отметим, что на данный момент имеют место быть отдельные случаи так называемой Балканизации ин-тернета (превращение глобальной сети Интернет во множество локальных сетей с искусственно уста-новленными государствами границами), как, например, в Китае с его «Великим Китайским файерво-лом». Попытки построения национального интернета есть и в России. Однако, данный феномен носит ограниченный характер и не получает пока глобального распространения.

[20] Занимал этот пост с 19 июля 2017 г. по 2 января 2019 г.

[21] Garamone J. Cybercom Now a Combatant Command, Nakasone Replaces Rogers [Electronic resource] / U.S. Department Of Defense. Washington, DC, 2018. May 4. Mode of access: https://www.defense.gov/Explore/News/Article/Article/1512994/cybercom-now-a-combatant-command-nakasone-replaces-rogers/ (date of access: 30.07.2020).

[22] Fischerkeller M. P., Harknett R. J. Deterrence is Not a Credible.... P. 382; Bebber R. There is No Such Thing as Cyber Deterrence. Please Stop [Electronic resource] / The Cipher Brief's Network. Washington, DC, 2018. Mode of access: https://www.thecipherbrief.com/column_article/no-thing-cyber-deterrence-please-stop (date of access: 31.07.2020).

В-третьих, в отличие от ядерного оружия, где существуют мощные научно-технологические и финансовые барьеры для входа в клуб ядерных держав, барьеры для обладания кибероружием в связи с *взаимосвязанным* киберпространством и низкой стоимостью технологий, отсутствуют[23], что делает сам факт конкуренции возможным для различных субъектов международных отношений. В-четвертых, в отличие от физических областей, киберпространство не может быть сегментировано на военную и гражданскую сферы, то есть в нём нельзя объявить или выделить отдельную зону военных действий, как в случае с сухопутным пространством[24].

Согласно военно-стратегической мысли Соединённых Штатов, все эти уникальные характеристики киберпространства определяют факт постоянного осуществления противниками таких кибератак против США, *которые нельзя квалифицировать как акт агрессии*[25].

В важнейшем стратегическом документе «Достижение и поддержание превосходства в киберпространстве: Руководство для Киберкомандования США» говорится, что из-за такой структурной особенности киберпространства, как взаимосвязанность, «противники постоянно осуществляют операции [против США. – С.А.], которые не достигают уровня вооружённого конфликта»[26]. В этом же документе сказано, что «киберпространство – это изменчивая среда постоянного контакта»[27].

То есть, согласно стратегическому мышлению Соединённых Штатов, то, что сегодня происходит в киберпространстве – это не киберконфликты и тем более не кибервойны, а долгосрочная согласованная стратегическая конкуренция между странами, так как кибероперации, которые происходят в условиях этой конкуренции, *не достигают уровня вооружённого конфликта.*

О том, что стратегическая конкуренция получает активное распространение именно в киберпространстве, напрямую было заявлено в «Киберстратегии Министерства обороны США», опубликованной в сентябре 2018 г. В ней открыто декларируется, что Соединённые Штаты уже сегодня *участвуют в этой долгосрочной*

Согласно военно-стратегической мысли США сегодня в киберпространстве происходят не военные киберконфликты, а долгосрочная согласованная стратегическая конкуренция

[23] Fischerkeller M. P., Harknett R. J. Deterrence is Not a Credible... P. 382; Nye J. S. Nuclear Lessons for Cyber Security [Electronic resource] / Strategic Studies Quarterly. 2011. Vol. 5, No. 4. P. 20, 22, 36. Mode of access: https://www.jstor.org/stable/26270536?seq=1#metadata_info_tab_contents (date of access: 31.07.2020).

[24] The United States of America Cyberspace Solarium Commission: Legislative Proposals [Electronic resource] / U.S. Cyberspace Solarium Commission. Washington, DC, 2020. P. 28. Mode of access: https://www.solarium.gov/report (date of access: 31.07.2020); Bebber R. There is No Such....

[25] Fischerkeller M. P., Harknett R. J. What Is Agreed...; Fischerkeller M. P., Harknett R. J. Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect [Electronic resource] / Lawfare. Washington, DC, 2020. Mode of access: https://www.lawfareblog.com/persistent-engagement-and-cost-imposition-distinguishing-between-cause-and-effect (date of access: 31.07.2020); Harknett R. J., Callaghan J. P., Kauff-man R. Leaving Deterrence Behind: WarFighting and National Cybersecurity [Electronic resource] / Journal of Homeland Security and Emergency Management. 2010. Vol. 7, No. 1. P. 15, 20 Mode of access: https://www.researchgate.net/publication/267224391_Leaving_Deterrence_Behind_War-Fighting_and_National_Cybersecurity (date of access: 31.07.2020); Nakasone P. M. A Cyber Force for Persis-tent Operations [Electronic resource] / Joint Force Quarterly. 2019. Vol. 92.. P. 11. Mode of access: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf (date of access: 31.07.2020); Bebber R. There is No Such...

[26] Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command [Electronic re-source] / U.S. Department of Defense. Washington, DC, 2018. P. 3. Mode of access: (date of access: 01.08.2020)https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf (date of access: 01.08.2020)

[27] Achieve and Maintain Cyberspace Superiority. P. 4.

стратегической конкуренции в киберпространстве, однако необходимость такого участия навязываются им их соперниками, которые постоянно осуществляют кибероперации, не достигающие уровня вооружённого конфликта, с целью нанести ущерб благосостоянию Америки[28]. Так, в стратегии сказано, что США ведут «*долгосрочную стратегическую конкуренцию с Китаем и Россией. Эти государства расширили [...] конкуренцию, включив в неё постоянные кампании в киберпространстве [...]* которые создают долгосроный стратегический риск для нации»[29]. Эта долгосрочная стратегическая конкуренция, в свою очередь, обуславливает потребность формирования уже Соединёнными Штатами *ежедневной киберконкуренции*, которая поможет им сохранить стратегическое превосходство в киберпространстве и противостоять киберугрозам[30].

Аналогичного мнения придерживаются и авторитетные американские эксперты в области кибербезопасности Ричард Харкнетт и Майкл Фишеркеллер, которые заявляют, что именно «противники США своим поведением формируют согласованную стратегическую конкуренцию в киберпространстве на уровне взаимодействия, где операционные эффекты не квалифицируются как вооружённое нападение»[31].

Важно отметить, в «Киберстратегии Министерства обороны США» от 2015 г. вообще не было упоминания о том, что Соединённым Штатам необходимо участвовать в долгосрочной стратегической конкуренции в киберпространстве. Сам термин «стратегическая конкуренция» также отсутствовал.

Ещё одним документом, в котором признается существование в киберпространстве стратегической конкуренции, а также обуславливается необходимость принятия в этих условиях новой стратегии действий в киберпространстве, является «Национальная киберстратегия Соединённых Штатов Америки», опубликованная в сентябре 2018 г. Так, в документе сказано следующее – «администрация признает, что *Соединённые Штаты ведут постоянную конкуренцию со стратегическими противниками [...]*»[32], и что «*это постоянная вовлечённость в киберпространстве уже меняет стратегический баланс сил*»[33].

Ещё один шаг в признании киберпространства ареной долгосрочной стратегической конкуренции великих держав был сделан в так называемом Отчёте комиссии по киберпространству «Солярий» (сущность которого будет раскрыта далее), опубликованном 11 марта 2020 г. В этом документе напрямую заявляется, что «*киберпространство уже является ареной стратегической конкуренции*, в которой государства проецируют свою мощь, за-

[28] The Department Of Defense Cyber Strategy 2018: Summary [Electronic resource] / U.S. Department of De-fense. Washington, DC, 2018. P. 1, 2. Mode of access: (date of access: 01.08.2020).https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (date of access: 01.08.2020).

[29] The Department Of Defense Cyber Strategy 2018. P. 1.

[30] The Department Of Defense Cyber Strategy 2018. P. 1, 4, 7.

[31] Fischerkeller M. P., Harknett R. J. Persistent Engagement, Agreed Competition, Cyberspace Interaction Dy-namics, and Escalation [Electronic resource] / Institute for Defense Analyses. Alexandria, Virginia, 2018. P. 9. Mode of access: https://pdfs.semanticscholar.org/832e/16cb7fcd6f732454b26ca86de31f2e8cd7c6.pdf?_ga=2.89625439.559095083.1578310623-1262708193.1578310623 (date of access: 02.08.2020).

[32] National Cyber Strategy of the United States of America [Electronic resource] / The White House. Washing-ton, DC, 2018. P. 2. Mode of access: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (date of access: 02.08.2020).

[33] National Cyber Strategy of the United States of America. P. 20.

щищают свои интересы и наказывают своих противников»[34].

И наконец, 20 октября 2020 г. Государственным департаментом США был опубликован документ «О международной безопасности в киберпространстве: новые модели для снижения рисков», согласно которому «возникновение новой эры конкуренции великих держав повысило ставки на кибер-арене»[35]. Таким образом, важность киберповестки в условиях стратегической конкуренции великих держав очевидна.

ПОЧЕМУ «ТРАДИЦИОННАЯ» СТРАТЕГИЯ КИБЕРСДЕРЖИВАНИЯ ОКАЗАЛАСЬ НЕЭФФЕКТИВНОЙ В УСЛОВИЯХ ДОЛГОСРОЧНОЙ СТРАТЕГИЧЕСКОЙ КОНКУРЕНЦИИ?

Итак, в новых условиях господства долгосрочной стратегической конкуренции великих держав в киберпространстве, операции в рамках которой *не достигают уровня вооружённого конфликта*, США решили, что доминировавшая долгое время стратегия киберсдерживания, основанная на *наказании* и *воспрещении*, оказалась неэффективной по двум причинам.

Во-первых, высшие военные и политические чины Соединённых Штатов пришли к выводу, что стратегия киберсдерживания *в её старом варианте (путём наказания)* подходит лишь для предотвращения тех *непостоянных* кибератак, которые *достигают* уровня вооружённого конфликта. Соответственно, в новых условиях долгосрочной стратегической конкуренции великих держав в киберпространстве, операции в рамках которой *не достигают уровня вооружённого конфликта*, эта стратегия киберсдерживания оказывается неэффективной. Например, в вышеупомянутом Отчёте Комиссии по киберпространству «Солярий» сказано, что, в то время как сдерживание было эффективно против кибератак со значительными последствиями, Соединённые Штаты не разработали никаких подходов для предотвращения тех киберугроз, *которые не достигают уровня вооружённого конфликта*[36]. Об этом говорится и в документе Кибернетического командования США «Достижение и поддержание превосходства в киберпространстве», согласно которому Соединённые Штаты «уступают [...] инициативу из-за длительных процессов одобрения [ответных мер. – С.А.], *которые [...] устанавливают очень высокий порог для реагирования на злонамеренные действия в киберпространстве*»[37].

Аналогичной позиции придерживаются и американские эксперты, среди которых Ричард Харкнетт, Майкл Фишеркеллер[38]. Так, они утверждают, что «центральная проблема для США заключается в стратегической конкуренции в киберпространстве, операции в рамках которой не достигают уровня воору-

США считают стратегию киберсдерживания, основанную на наказании и воспрещении, неэффективной, так как такой подход не решает проблему угроз, не достигающих уровня вооружённого конфликта, а также ставит страну в пассивную оборонительную позицию, тем самым предоставляя стратегическое преимущественно конкурентам США

[34] The United States of America Cyberspace Solarium Commission. P. 6.
[35] Ford C. A. International Security in Cyberspace: New Models for Reducing Risk [Electronic resource] / Arms Control and International Security Papers ;U.S. State Department. Washington, DC, 2020. Vol. I, No. 20. P. 1. Mode of access: (date of access: 20.10.2020).https://www.state.gov/wp-content/uploads/2020/10/T-paper-series-Cybersecurity-Format-508.pdf (date of access: 20.10.2020).
[36] The United States of America Cyberspace Solarium Commission. P. 24.
[37] Achieve and Maintain Cyberspace Superiority... P. 5.
[38] Fischerkeller M. P., Harknett R. J. Deterrence is Not a Credible.... P. 386; Fischerkeller M. P., Harknett R. J. Persistent Engagement and Tacit Bargaining...; Fischerkeller M. P., Harknett R. J. Persistent Engagement, Agreed Competition...; Fischerkeller M. P., Harknett R. J. What Is Agreed Competition...

жённого конфликта, и что стратегия сдерживания сама по себе не является эффективным подходом к обеспечению безопасности в этом стратегическом конкурентном пространстве»[39].

Во-вторых, стратегия киберсдерживания, основанная лишь на наказании и воспрещении, по мнению США, является *пассивным подходом*, так как в случае наказания предполагает осуществление ответных мер уже *постфактум*[40], а в случае воспрещения – ставит Соединённые Штаты в пассивную оборонительную позицию, что делает их на шаг позади своих противников и позволяет конкурентам оспаривать стратегические преимущества Америки в режиме реального времени[41].

Например, в документе «Достижение и поддержание превосходства в киберпространстве» утверждается, что противники Соединённых Штатов глубоко маневрируют в сетях США, «вынуждая правительство переходить в *режим реагирования после вторжений и атак*, которые дорого обходятся [США] [...] Эта *позиция, основанная на реагировании, представляет неприемлемый риск для [американских] систем [...]*»[42].

Таким образом, согласно экспертной и стратегической мысли США, устоявшаяся стратегия сдерживания киберугроз, базирующаяся чисто на двух методах – посредством наказания и воспрещения – неэффективна. Поэтому существующая концепция кибербезопасности нуждается в модернизации и принятии нового подхода (здесь отметим, что отказа от стратегии киберсдерживания как таковой не произошло).

Майкл Фишеркеллер и Ричард Харкнетт также утверждают, что «стратегия США при администрации Обамы предусматривала сдерживание путём воспрещения и [...] сдерживание путём введения затрат [...] К сожалению, учитывая уникальные характеристики домена, сдерживание не является надежной стратегией для киберпространства»[43]. Аналогичного мнения придерживается и капитан-лейтенант ВМФ США Роберт «Джейк» Беббер, заявивший, что Соединённые Штаты «не смогли оценить уникальные характеристики киберпространства как стратегической среды [...] и вместо этого применили систему ядерного сдерживания»[44].

Как сказано в «Национальной киберстратегии Соединённых Штатов Америки» от 2018 г., «новые угрозы и новая эра стратегической конкуренции требуют новой кибер-стратегии, которая отвечает новым реалиям [...]»[45].

НОВЫЙ ПОДХОД В ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ США: ПОСТОЯННАЯ ВОВЛЕЧЁННОСТЬ В КИБЕРПРОСТРАНСТВЕ

[39] Fischerkeller M. P., Harknett R. J. Persistent Engagement and Tacit Bargaining.
[40] The United States of America Cyberspace Solarium Commission. P. 24; Libicki M. C. It Takes More.... P. 2; Goldman E. O. From Reaction to Action...
[41] Achieve and Maintain Cyberspace Superiority... P. 5, 6; The United States of America Cyberspace Solarium Commission. P. 24; Nakasone P. M., Sulmeyer M. How to Compete in Cyberspace [Electronic resource] / For-eign Affairs. New York, NY, 2020. Mode of access: https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity (date of access: 30.08.2020); Bebber R. There is No Such...; Fischerkeller M. P., Harknett R. J. What Is Agreed...; Harknett R.J. Progress Is the Promise...; Harknett R. J., Callaghan J. P., Kauffman R. Leaving Deterrence Behind... P. 15, 20; Sulmeyer M. How the U.S. Can Play Cyber-Offense.
[42] Achieve and Maintain Cyberspace Superiority... P. 5.
[43] Fischerkeller M.P., Harknett R.J. Deterrence is Not a Credible... P. 385.
[44] Bebber R. There is No Such...
[45] National Cyber Strategy of the United States of America. P. 2.

В связи с вышесказанным, Соединённые Штаты пришли к выводу, что им нужна новая стратегия действий в киберпространстве – стратегия *постоянной вовлечённости*.

Постоянная вовлечённость (от англ. – «persistent engagement») – это постоянное осуществление упреждающих кибероперaций, которые не достигают уровня вооружённого конфликта, в режиме реального времени против потенциальных противников как можно ближе к источнику предполагаемой агрессии, с целью навязать им дополнительные стратегические затраты, оспорить их превосходство и в то же время подтвердить стратегическое превосходство США в киберпространстве.

Важно отметить, что стратегия постоянной вовлечённости является инструментом для реализации так называемой *упреждающей защиты* (от англ. – «*defend forward*»)[46], подразумевающей проведение упреждающих кибероперaций *в сетях противника* на постоянной основе, и, в случае необходимости – выведение из строя систем и серверов противника *ещё до того, как он осуществит кибератаки*[47]. Так, Министерство обороны США придерживается мнения о том, что «оборонительные» действия могут быть упреждающими только при осуществлении постоянной вовлечённости[48].

Важно перечислить ключевые составляющие элементы стратегии постоянной вовлечённости:

1) Постоянное осуществление кибероперaций в отношении потенциальных противников, или постоянный контакт с противником (от англ. – «*persistent contact*», или «*constant contact*»)[49].
2) Кибероперации, осуществляемые при постоянной вовлечённости, ни в коем случае не достигают уровня вооружённого конфликта[50].

[46] The United States of America Cyberspace Solarium Commission. P. 111, 137, 162; Schneider J. G. Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy [Electronic resource] // Lawfare. Washing-ton, DC, 2019. Mode of access: https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy (date of access: 12.07.2020); Nakasone P. M., Sulmeyer M. How to Compete in Cy-berspace.

[47] The Department Of Defense Cyber Strategy 2018; The United States of America Cyberspace Solarium Com-mission. P. 6, 24, 25, 28-30; Sulmeyer M. How the U.S. Can Play Cyber-Offense; Jasper S. Strategic Cyber Deterrence...

[48] The United States of America Cyberspace Solarium Commission. P. 111, 137, 162; Schneider J. G. Persistent Engagement...

[49] The United States of America Cyberspace Solarium Commission. P. 162; Fischerkeller M. P., Harknett R. J. Deterrence is Not a Credible... P. 391; Fischerkeller M. P., Harknett R. J. Persistent Engagement, Agreed Com-petition... P. 3; Nakasone P. M., Sulmeyer M. How to Compete in Cyberspace.

[50] The Department Of Defense Cyber Strategy 2018... P. 2; Achieve and Maintain Cyberspace Superiority... P. 6; Fischerkeller M. P., Harknett R. J. Persistent Engagement, Agreed Competition...P. 2, 21, 22; Fischerkeller M. P., Harknett R. J. What Is Agreed Competition in Cyberspace?

3) Цель применения Вашингтоном стратегии постоянной вовлечённости – создать «тактические препятствия» (от англ. – «*tactical friction*») и наложить стратегические издержки на противников Соединённых Штатов[51].
4) Операции, осуществляемые в рамках постоянной вовлечённости, являются *упреждающими*.

Новая стратегия постоянной вовлечённости впервые была изложена в уже упомянутом важнейшем стратегическом документе Кибернетического командования США «Достижение и поддержание превосходства в киберпространстве: Руководство для Киберкомандования США», опубликованном 23 марта 2018 г.

Наиболее важной чертой стратегии постоянной вовлеченности является проведение тактических операций, которые не приводят к вооружённому конфликту, а только создают препятствия противнику в киберпространстве

Во-первых, в данном руководстве неоднократно утверждается, что противники Соединённых Штатов постоянно осуществляют против них кибероперации, *которые не достигают уровня вооружённого конфликта*, чтобы получить конкурентные преимущества над США[52], а киберпространство является «изменчивой средой постоянного контакта», в котором непрерывно оспаривается стратегическое превосходство и в котором оборона всегда будет подвергаться испытаниям на прочность[53].

Во-вторых, в соответствии с этим, Соединённые Штаты будут постоянно осуществлять упреждающие кибероперации, не достигающие уровня вооружённого конфликта, максимально близко к источнику предполагаемой агрессии, тем самым «изматывая» противника, создавая тактические препятствия и сокращая вражеские кибератаки, заставляя его сосредотачиваться на обороне собственных систем[54]. При этом, осуществляя операции в киберпространстве, США собираются «маневрировать между защитой и нападением»[55]. Особое внимание следует обратить на то, что эти операции также будут упреждающими – в «Руководстве» неоднократно заявляется, что США намерены предотвращать вражеские атаки *ещё до того, как они достигнут американских систем и сетей*[56] – то есть, до того, как они будут запущены, учитывая то, что кибератаки носят мгновенный характер. Документ предусматривает регулярное вторжение в сети противника с целью проведения в них подрывных операций и выявления его слабых сторон, изучения его намерений и возможностей[57]. Вот что по этому поводу говориться в самом документе: «Мы [США. – С.А.] будем *преследовать злоумышленников во всех сетях и системах*, чтобы сделать большинство злонамеренных кибер-действий неэффективными»[58].

Именно так выглядит стратегия постоянной вовлечённости в данном «Руководстве», согласно которому, цель такого операционного подхода – создание тактических препятствий и на-

[51] Achieve and Maintain Cyberspace Superiority... P. 6; The United States of America Cyberspace Solarium Commission. P. 6, 24; Fischerkeller M. P., Harknett R. J. Persistent Engagement, Agreed Competition... P. 4; Fischerkeller M. P., Harknett R. J. Persistent Engagement and Cost Imposition; Harknett R. J. United States Cyber Command's New Vision: What It Entails and Why It Matters [Electronic resource] / Lawfare. Washing-ton, DC, 2018. Mode of access: https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters (date of access: 06.08.2020).
[52] Achieve and Maintain Cyberspace Superiority... P. 2, 3.
[53] Achieve and Maintain Cyberspace Superiority... P. 4, 6
[54] Achieve and Maintain Cyberspace Superiority... P. 1, 2, 4, 6, 7; Nakasone P. M. A Cyber Force for Persistent Operations.
[55] Achieve and Maintain Cyberspace Superiority... P. 6.
[56] Achieve and Maintain Cyberspace Superiority... P. 1, 2, 5, 6.
[57] Achieve and Maintain Cyberspace Superiority...
[58] Achieve and Maintain Cyberspace Superiority... P. 6.

ложение стратегических издержек на противников Соединённых Штатов[59]. Применяя стратегию постоянной вовлечённости, США будут удерживать долгосрочное стратегическое преимущество и оперативное превосходство в киберпространстве, которое теперь является «взаимосвязанным пространством боевых действий»[60].

Принятие нового стратегического подхода постоянной вовлечённости нашло своё отражение в другом стратегическом документе – «Киберстратегии Министерства обороны США», опубликованном в сентябре 2018 г.

Как уже было сказано, в «Киберстратегии» обуславливается необходимость формирования Соединёнными Штатами *ежедневной киберконкуренции*, которая поможет им сохранить стратегическое превосходство в киберпространстве и противостоять киберугрозам[61].

Стратегия постоянной вовлечённости в документе сформулирована следующим образом – США будут «*проводить операции в киберпространстве*» и прибегнут к «*упреждающей защите, чтобы воспрепятствовать или остановить злонамеренную кибер-активность прямо в её источнике, включая ту деятельность, которая не достигает уровня вооружённого конфликта*»[62].

Таким образом, в «Киберстратегии» говорится о важности осуществления именно упреждающей защиты, которая позволит им осуществлять кибероперации *как можно ближе к источнику злонамеренной активности* с целью противодействия киберугрозам[63] ещё *до того, как вражеские кибератаки достигнут своей цели*[64].

Важно отметить, что в рассматриваемой стратегии наблюдается существенная эволюция в подходах к обеспечению кибербезопасности относительно предыдущей «Киберстратегии Министерства обороны США» от 2015 г. Так, Киберстратегия от 2018 г. резко изменила стратегический подход со стратегии сдерживания киберугроз путём наказания и воспрещения, которая была доминирующей в «Киберстратегии Министерства обороны США» от 2015 г., на участие в долгосрочной стратегической конкуренции в киберпространстве. Как и в случае с термином «стратегическая конкуренция», термин «постоянная вовлечённость» также полностью отсутствовал в Киберстратегии от 2015 г. Это же касается и концепции упреждающей защиты, которая тоже не упоминалась в прошлой стратегии.

КАК ПОСТОЯННАЯ ВОВЛЕЧЁННОСТЬ СТАЛА ЧАСТЬЮ РАСШИРЕННОГО КИБЕРСДЕРЖИВАНИЯ

Наравне с принятием новой операционной модели постоянной вовлечённости киберсдерживание не утратило своих позиций. Например, в «Руководстве для Киберкомандования США» – главном стратегическом документе Киберкомандования, который провозгласил постоянную вовлечённость в качестве нового операционного подхода – вместе в этим заявляется, что Киберкомандование США и дальше «будет способствовать [...] национальному стратегическому сдерживанию»[65].

Более основательная попытка примирить два, на первый

[59] Achieve and Maintain Cyberspace Superiority... P. 6
[60] Achieve and Maintain Cyberspace Superiority... P. 4, 6, 7.
[61] The Department Of Defense Cyber Strategy 2018... P. 1, 4, 7.
[62] The Department Of Defense Cyber Strategy 2018... P. 1.
[63] The Department Of Defense Cyber Strategy 2018... P. 1, 2, 4, 7.
[64] The Department Of Defense Cyber Strategy 2018... P. 2.
[65] Achieve and Maintain Cyberspace Superiority... P. 7.

взгляд, взаимоисключающих подхода, была сделана в «Киберстратегии Министерства обороны США» 2018 г., где наравне со стратегической конкуренцией декларируется и стратегия киберсдерживания. Как уже было сказано выше, новая операционная модель постоянной вовлечённости должна эффективно противодействовать кибератакам, которые не достигают уровня вооружённого конфликта, в то время как сдерживание может быть эффективно лишь против тех кибератак, которые, соответственно, квалифицируются как акт агрессии. Так, в Киберстратегии сдерживание киберугроз и постоянная вовлечённость выступают в качестве двух *взаимоусиливающих* подходов[66]. Согласно документу, Соединённые Штаты прибегнут к сдерживанию тех «злонамеренных действий в киберпространстве, *которые представляют собой применение силы* против Соединённых Штатов», и будут «постоянно противодействовать *злонамеренной киберактивности в ежедневных соревнованиях*»[67]. Исходя из содержания Киберстратегии, взятые вместе, сдерживание и постоянная вовлечённость в качестве *взаимодополняющих действий* позволят Министерству обороны конкурировать, сдерживать и побеждать противников в киберпространстве[68].

Приверженность киберсдерживанию сохраняется и в «Национальной киберстратегии Соединённых Штатов Америки», опубликованной в сентябре 2018 г. Так, среди прочего, она описывает, как Соединённые Штаты будут обеспечивать безопасность путем *совершенствования способности сдерживать и наказывать тех*, кто использует киберинструменты в злонамеренных целях[69]. С самого начала в стратегии говорится, что «у Соединённых Штатов также должна быть политика для наложения издержек, если они надеются *сдержать* злонамеренных кибер-субъектов и предотвратить дальнейшую эскалацию»[70].

В стратегии ясно прописывается, что США будут «сдерживать злонамеренных киберсубъектов путём наложения на них и их спонсоров затрат за счет использования целого ряда инструментов, включая, помимо прочего, судебное преследование и экономические санкции, в рамках более *широкой стратегии сдерживания*»[71]. Как можно видеть, в стратегии сдерживание киберугроз в основном базируется на уже знакомом принципе наложения затрат и издержек. Несмотря на это, стратегия предполагает сдвиг в политике обеспечения кибербезопасности к более проактивной и даже наступательной позиции[72]. Например, согласно стратегии, Министерство обороны совместно с правоохранительными органами получают право *совершать наступательные действия в киберпространстве*.

[66] The Department Of Defense Cyber Strategy 2018... P. 4.
[67] The Department Of Defense Cyber Strategy 2018... P. 4.
[68] The Department Of Defense Cyber Strategy 2018... P. 4, 7.
[69] National Cyber Strategy of the United States of America. P. 2, 3.
[70] National Cyber Strategy of the United States of America. P. 2.
[71] National Cyber Strategy of the United States of America. P. 8.
[72] Смекалова М. Зажмуриться и действовать: кибериторги 2018 года // Российский совет по международ-ным делам : сайт. 2018. URL: https://russiancouncil.ru/2019-globalissues#2 (дата обращения: 09.08.2020).

Исходя из того факта, что в описанных документах присутствует и постоянная вовлечённость, и киберсдерживание, можно предположить, что они не просто рассматриваются военно-политическим руководством США в качестве взаимодополняющих подходов, но и что постоянная вовлечённость, возможно, рассматривается как абсолютно новый подход в рамках того же сдерживания, только теперь уже расширенного.

Ещё раз напомним, что разница между киберсдерживанием в том виде, в каком оно осуществлялось в период президентства Барака Обамы[73], и постоянной вовлечённостью в киберпространстве состоит в том, что «классическое» *киберсдерживание направлено только против тех непостоянных кибератак, которые можно квалифицировать как акт агрессии*, а цель постоянной вовлечённости – в режиме реального времени на основе постоянного контакта с противником в киберпространстве противодействовать тем киберугрозам, которые *не достигают уровня вооружённого конфликта, что делает саму постоянную вовлечённость малопригодной для предотвращения кибератак, приравниваемых к вооружённому конфликту*. Также, принятие на вооружение лишь постоянной вовлечённости в киберпространстве и отказ от стратегии киберсдерживания сразу же исключает из всего спектра возможных вариантов предотвращения киберугроз такие важные варианты, как ответные меры – начиная с традиционных военных, и заканчивая дипломатическими, экономическими, правовыми мерами и т.д. Значит, стратегия киберсдерживания будет оставаться эффективной стратегией для предотвращения особо опасных кибератак.

Задача по объединению эффектов стратегии постоянной вовлечённости и стратегии киберсдерживания была взята на себя так называемой Комиссией по киберпространству «Солярий», созданной для исполнения соответствующих положений «Национального закона им. Джона С. Маккейна о государственной обороне на 2019 финансовый год» с целью «*выработки консенсуса касательно стратегического подхода к защите Соединённых Штатов в киберпространстве от кибератак со значительными последствиями*»[74]. Как видно из цитаты, задача Комиссии состояла именно в выработке консенсуса между двумя конкурирующими подходами к обеспечению кибербезопасности США.

Комиссия по киберпространству «Солярий» была со-

[73] Так о сдерживании говорилось в докладе комиссии по кибербезопасности Центра стратегических и международных исследований под названием «От осведомленности к действию: программа действий для 45-ого президента США». См. From Awareness to Action: A Cybersecurity Agenda for the 45th Presi-dent: A Report of the CSIS Cyber Policy Task Force [Electronic resource] / Center for Strategic and International Studies. Washington, DC, 2017. P. 4. URL: http://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf (date of access: 10.08.2020).

[74] John S. McCain National Defense Authorization Act for Fiscal Year 2019: Conference Report to Accompany H.R. 5515[Electronic resource] / House of Representatives. 115th Congress 2d Session. Washington, DC, 2018. P. 23, 1170, 1276-1292. Mode of access: https://docs.house.gov/billsthisweek/20180723/CRPT-115hrpt863.pdf (date of access: 10.08.2020).

здана по образу проекта «Солярий» 1953 г., в рамках которого тремя целевыми группами было разработано соответственно три конкурирующих стратегии противостояния Советскому Союзу: 1) международное сдерживание на основе развития военно-союзнических отношений со странами Европы; 2) сдерживание с опорой на собственные военные силы Соединённых Штатов, и прежде всего – на ядерное оружие; 3) стратегия «возврата в исходное положение», цель которой – «отбрасывание коммунизма» и уменьшение общего влияния СССР на мировой арене. Однако, в отличие от проекта «Солярий» 1953 г., в рамках которого вышеописанные стратегии создавались как конкурирующие[75], проект «Киберсолярий» объединил в одной концепции наработки всех групп, работающих более или менее независимо.

Отчёт Комиссии по киберпространству «Солярий» показал военно-политическому руководству США, как могут соотносится друг с другом постоянная вовлечённость и сдерживание, предоставив подход многоуровневого киберсдерживания

Можно предположить, что в своём рекомендательном Отчёте, опубликованном 11 марта 2020 г., Комиссия по киберпространству «Солярий» пришла к выводу о необходимости не только разработать механизмы предотвращения кибератак, *не достигающих уровня вооружённого конфликта*, но и объединить сформировавшиеся к этому моменту конкурирующие стратегии – сдерживание киберугроз, продвижение международных норм и постоянную вовлечённость – в одном универсальном подходе. Эксперты, вошедшие в состав комиссии, стали анализировать противоречия, существующие в концепции кибербезопасности из-за совершенно разных подходов, а также изучать то, как США могли бы наилучшим образом унифицировать все эти подходы в одной стратегии. В результате этих усилий в Отчёте Комиссии по киберпространству «Солярий» постоянная вовлечённость оказалась «растворена» в объединённой стратегии, которая получила название «*многоуровневое киберсдерживание*» (от англ. – «*layered cyber deterrence*»)[76]. Данная стратегия, согласно Отчёту, включает в себя три уровня: 1) продвижение международных норм; 2) лишение выгод; 3) наложение издержек.

Собственно, постоянная вовлечённость и киберсдерживание, основанное на наказании, были объединены в подходе, который получил название «наложение издержек» (от англ. – «*impose costs*»), а именно включены в 3-ий уровень как взаимодополняющие стратегии[77]. Исходя из вышеописанной логики, можно сделать вывод, что объединение в рамках одного подхода двух ранее конкурирующих стратегий преследует главную цель – синергировать их потенциал: *«традиционного» киберсдерживания* – для предотвращения тех киберугроз, *которые можно квалифицировать как акт агрессии*, и *постоянной вовлечённости – для противодействия киберугрозам, которые не достигают уровня вооружённого конфликта*. Очень важным компонентом многоуровневого сдерживания в Отчёте является упреждающая защита, которая «включает упреждающее и комплексное использование всех инструментов власти», и «требует, чтобы Соединённые Штаты обладали способностями и возможностями для постоянной вовлечённости в киберпространстве с целью наложения на противников издержек за их злонамеренную кибердеятельность»[78].

[75] В итоге, по приказу Д. Эйзенхауэра наработки проекта «Солярий» были переданы в специальную группу Совета национальной безопасности США, в результате чего «всё лучшее» из трёх конкурирующих под-ходов было объединено в документе СНБ 162/2, основу которого как раз и составляли разработки про-екта «Солярий». Однако сами эксперты, работавшие в разных группах, изначально не были согласны объединять разработанные ими по отдельности стратегии.

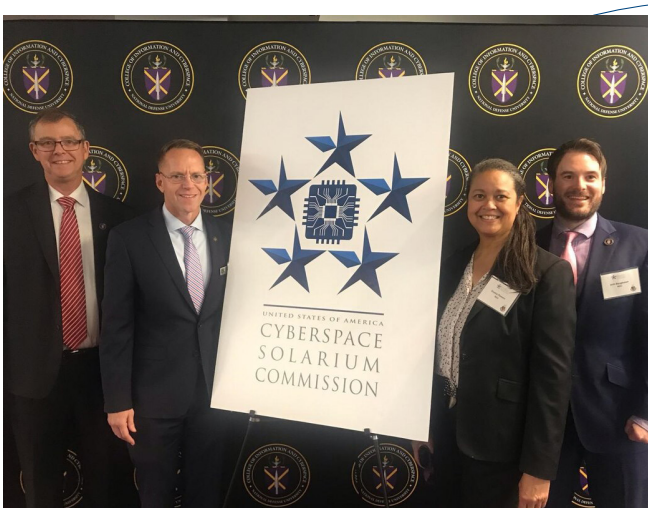
[76] The United States of America Cyberspace Solarium Commission. P. 1, 2, 7, 23-30.

[77] The United States of America Cyberspace Solarium Commission. P. 6, 24-25.

[78] The United States of America Cyberspace Solarium Commission. P. 24-25, 29.

Таким образом, подход, сформулированный в Отчёте – *многоуровневое киберсдерживание* – предусматривает использование всех инструментов национальной власти – как военных, включающих в себя ответные меры, постоянную вовлечённость и упреждающую защиту, так и судебных, экономических, дипломатических и т.д., тем самым расширяя спектр возможных вариантов предотвращения киберугроз *разного* уровня – как достигающих порога вооружённого конфликта, так и не достигающих[79].

Именно Отчёт Комиссии по киберпространству «Солярий» показал военно-политическому руководству США, как могут соотносится друг с другом постоянная вовлечённость и сдерживание. При этом, представленный подход – многоуровневое киберсдерживание – может являться своего рода «расширенным» сдерживанием, которое постоянно развивается и включает в себя всё новые инструменты. Как сказано в самом Отчёте – «стратегические дискуссии слишком часто отдают предпочтение узким определениям сдерживания, которые не учитывают то, как технологии меняют общество»[80].



Комиссия по киберпространству «Солярис»

Источник: www.civilsociety.co.uk

Из рассмотрения вышеописанных документов можно сделать вывод, что постоянная вовлечённость может рассматриваться военно-политическим руководством Соединённых Штатов как новая составляющая расширенного сдерживания. Эта новая стратегия постоянной вовлечённости нужна США именно для того, чтобы предотвращать те киберугрозы, на которые не распространяется спектр действия киберсдерживания – то есть на киберугрозы, не достигающие уровня вооружённого конфликта. В дополнение к этому, несмотря на то что акцент всё сильнее стал смещаться на постоянную вовлечённость в киберпространстве, стратегия киберсдерживания путём наказания и воспрещения не была исключена из концепции кибербезопасности США. Более того, стратегия постоянной вовлечённости в киберпространстве и стратегия киберсдерживания могут рассматриваться как взаимодополняющие стратегии.

Тем не менее, принятие нового стратегического подхода, пусть и в рамках «расширенного» сдерживания, потребовало определённых изменений для своей реализации на практике.

ИНСТИТУЦИОНАЛЬНЫЕ И ПОЛИТИКО-ПРАВОВЫЕ ИЗМЕНЕНИЯ, ПОЗВОЛЯЮЩИЕ ПРИМЕНЯТЬ НА ПРАКТИКЕ СТРАТЕГИЮ ПОСТОЯННОЙ ВОВЛЕЧЁННОСТИ

Произошедшие концептуальные изменения сопровождались реальной эволюцией военно-политических институтов и изменением соответствующей политики с той

[79] The United States of America Cyberspace Solarium Commission. P. 6.
[80] The United States of America Cyberspace Solarium Commission. P. 23.

Генерал-лейтенант армии Пол Накасоне, глава Киберкомандования США, приносит присягу перед Комитетом по разведке Сената (Вашингтон, США, 15 марта 2018 г.)

Источник: www.reuters.com

В 2018 г. Киберкомандование США стало десятым полноценным объединенным боевым командованием США

целью, чтобы новая стратегия постоянной вовлечённости могла быть реализована на практике.

Что касается сугубо институциональных изменений, то главное, на что необходимо обратить внимание – это выделение Кибернетического командования США, которое было создано Бараком Обамой 23 июня 2009 г. и попало в подчинение Стратегического командования США[81], в отдельную и полностью самостоятельную структуру. Таким образом, статус Киберкомандования был повышен до полноценного объединенного боевого командования – десятого по счёту – что поставило его в один ряд с девятью другими боевыми командованиями США, о чём было заявлено 4 мая 2018 г.[82] Указ же об этом был подписан президентом Дональдом Трампом ещё раньше – в августе 2017 г.[83]

Закономерность данного институционального изменения проявляется в следующем. Экстраполируя стратегию *ядерного* сдерживания на киберугрозы, США оставались в плену представлений, сформированных в эпоху Холодной войны. Соответственно, нет ничего удивительного в том, что, следуя логике принятия стратегии сдерживания теперь уже киберугроз, Киберкомандование сначала попало в подчинение Стратегического командования США, которое контролирует именно ядерные силы Соединённых Штатов[84]. Выделение Киберкомандования в самостоятельную единицу в составе Пентагона, как представляется, точно так же является институциональным отражением принятия стратегии постоянной вовлечённости – получение Киберкомандованием «самостоятельности» не только предоставляет ему соответствующие полномочия по претворению постоянной вовлечённости в жизнь, но и отход от «традиционного и устаревшего» киберсдерживания.

Ещё одно событие, не только отражающее и легитимизирующее происходящие концептуальные изменения, но и демонстрирующее то, что стратегия постоянной вовлечённости принимается на вооружение и нуждается в определённых институтах для её реализации, произошло в апреле 2019 г., когда было объявлено, что так называемая Целевая группа Агентства национальной безопасности (АНБ) и Киберкомандования США (распространённое название – «Российская малая группа», от англ. – *Russian Small Group*, или RSG), созданная ещё в июле 2018 г. специально для противодействия кибератакам и «вмешательству» России в промежуточные выборы США 2018 г. с «ограниченным» сроком

[81] William J. DOD creates Cyber Command as U.S. Strategic Command subunit [Electronic resource] /
The Business of Federal Technology. McLean, VA, 2009. Mode of access: (date of access: 13.08.2020).https://fcw.com/Articles/2009/06/24/DOD-launches-cyber-command.aspx (date of access: 13.08.2020).

[82] Garamone J. Cybercom Now...; Strobel W. Pentagon's Cyber Command gets upgraded status, new leader [Elec-tronic resource] / Reuters. 2018. Mode of access: https://www.reuters.com/article/us-usa-defense-cyber/pentagons-cyber-command-gets-upgraded-status-new-leader-idUSKBN1I52MS (date of access: 13.08.2020); Spoehr T., Pane J. D. Elevating Cyber Command: An Overdue Step Towards Enhancing Military Cyber Operations [Electronic resource] / The Heritage Foundation. Washington, DC, 2018. Mode of access: https://www.heritage.org/cybersecurity/commentary/elevating-cyber-command-overdue-step-towards-enhancing-military-cyber (date of access: 13.08.2020).

[83] Statement by President Donald J. Trump on the Elevation of Cyber Command [Electronic resource] // The White House. Washington, DC, 2017. Mode of access: https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/ (date of access: 14.08.2020).

[84] William J. DOD creates Cyber Command...

работы[85], *теперь является постоянно действующим подразделением*[86]. Это было сделано на фоне заявлений Белого Дома о том, что кибероперации из России превратились в постоянную угрозу[87]. Таким образом, превращение Российской малой группы в постоянно действующее подразделение отражает тот факт, что стратегия постоянной вовлечённости также принимается Соединёнными Штатами на довольно долгосрочную перспективу.

Что касается политико-правовых изменений, то важнейшим событием, создавшим почву для осуществления стратегии постоянной вовлечённости на практике, стало подписание 16 августа 2018 г. Дональдом Трампом нового Президентского меморандума о национальной безопасности № 13 «О наступательных кибероперациях» (от англ. – «*National Security Presidential Memorandum 13*», или NSPM 13). Данный документ полностью засекречен и его точное название неизвестно[88]. Однако, как говорят сторонние источники, данный указ существенно расширяет возможности и условия применения кибероружия против потенциальных противников США *в наступательных целях*, отменив предыдущую аналогичную политическую директиву президента США № 20: «Политика США в отношении кибер-операций» (от англ. – «*Presidential Policy Directive 20: U.S. Cyber Operations Policy*», или PPD-20), которая была подписана ещё Бараком Обамой и предполагала некоторые ограничения при осуществлении кибероперации, а также регламентировала порядок применения кибероружия в отношении противников Соединённых Штатов[89].

Таким образом, новый президентский меморандум даёт начало развитию важнейшего принципа – *возможности активного осуществления наступательных действий в киберпространстве*, в том числе и упреждающих, для предотвращения киберугроз, *не достигающих уровня вооружённого конфликта.*

Ещё одно важнейшее изменение в 2018 г. коснулось уже упомянутого ранее «Национального закона им. Джона С. Маккейна о государственной обороне на 2019 финансовый год» (от англ. – «*National Defense Authorization Act for Fiscal Year 2019*», или «NDAA»). В новой редакции закона были сняты ограничения на осуществление некоторых видов кибероперации, которые ранее квалифицировались как «тайные», а теперь были приравнены к

Президентский меморандум о национальной безопасности № 13 «О наступательных кибероперациях» от 16 августа 2018 г. предоставил возможность активного осуществления наступательных действий в киберпространстве, в том числе и упреждающих, для предотвращения киберугроз, не достигающих уровня вооружённого конфликта

[85] Lyngaas S. NSA chief confirms he set up task force to counter Russian hackers [Electronic resource] / Cyber-scoop. Washington, DC, 2018. Mode of access: (date of access: 15.08.2020).https://www.cyberscoop.com/russia-small-group-paul-nakasone-nsa-aspen/ (date of access: 15.08.2020).

[86] Vavra S. SA's Russian cyberthreat task force is now permanent [Electronic resource] / Cyberscoop. Washing-ton, DC, 2019. Mode of access: https://www.cyberscoop.com/nsa-russia-small-group-cyber-command/ (date of access: 15.08.2020).

[87] Barnes J. E., Goldman A. F.B.I. Warns of Russian Interference in 2020 Race and Boosts Counterintelligence Operations [Electronic resource] / The New York Times. New York, NY, 2019. Mode of access: https://www.nytimes.com/2019/04/26/us/politics/fbi-russian-election-interference.html (date of access: 15.08.2020).

[88] National Security Presidential Memoranda [NSPMs] [Electronic resource] / Federation of American Scientist. Washington, DC. Mode of access: https://fas.org/irp/offdocs/nspm/index.html (date of access: 17.08.2020).

[89] Volz D. Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive [Electronic resource] / The Wall Street Journal. New York, NY, 2018. Mode of access: (date of access: 17.08.2020); Зинченко А. В., Толстухина А. Ю. Мир или война в киберпространстве? [Электронный ресурс] / Международная жизнь. 2018. № 9. С. 85 Mode of access: http://www.intelros.ru/pdf/Mezdunarodnaya_gizn/2018-09/8.pdf (дата обращения: 17.08.2020); Смекалова М. Зажмуриться и действовать: киберитоги 2018 года...-1534378721 (date of access: 17.08.2020); Зинченко А. В., Толстухина А. Ю. Мир или война в киберпро-странстве? // Международная жизнь. 2018. № 9. С. 85. URL:: http://www.intelros.ru/pdf/Mezdunarodnaya_gizn/2018-09/8.pdf (дата обращения: 17.08.2020); Смекалова М. Зажмуриться и действовать...

«*традиционной* военной деятельности»[90]. Это нововведение позволило Министерству обороны США проводить кибероперации и преследовать злоумышленников вне «национальных» сетей.

Как можно видеть, кибероперации, которые никогда не квалифицировались как «традиционные», теперь по своему концептуальному статусу стали именно таковыми. Это важнейшее изменение. Во-первых, оно отражает процесс происходивших в концепции кибербезопасности США трансформаций с юридической точки зрения и «на бумаге». Во-вторых, оно отражает процесс этих трансформаций с практической точки зрения, «развязав руки» Киберкомандованию США и позволив им осуществлять наступательные кибероперации на законных основаниях.

Военные США позитивно восприняли данные изменения, фактически заявив, что благодаря снятию некоторых правовых ограничений у них появилось больше возможностей для осуществления широкого спектра операций в киберпространстве[91]. Однако выдающийся эксперт в области кибербезопасности Джейсон Хили утверждает, что стратегия постоянной вовлечённости позволяет военным требовать всё больших полномочий, снятия ограничений на определённые действия и постоянного повышения оборонного бюджета[92].

Итак, все вышеописанные политико-институциональные изменения предоставляют прочную основу для реализации стратегии *постоянной вовлечённости.*

ПОСТОЯННАЯ ВОВЛЕЧЁННОСТЬ КАК СПОСОБ ФОРМИРОВАНИЯ ПРАВИЛ ПРИЕМЛЕМОГО ПОВЕДЕНИЯ В КИБЕРПРОСТРАНСТВЕ

Согласно новому стратегическому мышлению Вашингтона, стратегия постоянной вовлечённости автоматически решает проблему международного сотрудничества и принятия всеми сторонами согласованных и универсальных правил поведения государств в киберпространстве, по вопросу единогласного признания и исполнения которых всеми государствами существенных перспектив пока не наблюдается[93]. Так, по мнению Майкла Фишеркеллера и Ричарда Харкнета, стратегический подход к разработке норм в киберпространстве, основанный на дипломатии, как и стратегия киберсдерживания, точно так же не учитывает уникальные характеристики киберпространства[94].

По мнению и самого Пентагона, постоянная вовлечённость в киберпространстве позволит прояснить

[90] John S. McCain National Defense...P. 1232.

[91] Pomerleau M. Defense officials taking advantage of new cyber authorities [Electronic resource] / Fifth Do-main. Tysons, Virginia, 2018. Mode of access: https://www.fifthdomain.com/dod/cybercom/2018/11/27/defense-officials-taking-advantage-of-new-cyber-authorities/ (date of access: 19.08.2020); Pomerleau M. Is Cyber Command really being more 'aggressive' in cyberspace? [Electronic resource] / Fifth Domain. Tysons, Virginia, 2019. Mode of access: https://www.fifthdomain.com/dod/2019/04/25/is-cyber-command-really-being-more-aggressive-in-cyberspace/ (date of access: 19.08.2020).

[92] Healey J. The implications of persistent (and permanent) engagement in cyberspace [Electronic resource] / Journal of Cybersecurity. 2019. Vol. 5, Issue 1. Mode of access: https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878 (date of access: 19.08.2020).

[93] Искомые правила поведения уже давно принимаются в рамках ООН, однако они носят необязательный характер и не всегда исполняются.

[94] Fischerkeller M. P., Harknett R. J. Deterrence is Not a Credible... P. 383.

различие между приемлемым и неприемлемым поведением в киберпространстве, и, следовательно, будет способствовать большей стабильности и безопасности[95].

Возникает вопрос – каким образом осуществление кибероперaций в режиме реального времени, не достигающих уровня вооружённого конфликта, то есть постоянная вовлечённость, может привести различные стороны к пониманию приемлемого поведения в киберпространстве?

Американская стратегическая мысль даёт неординарный ответ на этот вопрос. Предполагается, что в ходе постоянной вовлечённости конкурирующие стороны будут осуществлять кибероперации разной мощности и интенсивности. Какие-то кибератаки будут рассматриваться как теоретически допустимые, в то время как другие потребуют сигнализации о их недопустимости с помощью незамедлительных ответных мер (например – моментального отключения сервера противника, с которого осуществлялась кибератака). Таким образом, постепенно будет приходить понимание того, что приемлемо, а что – нет, и правила приемлемого поведения выработаются автоматически за счёт постепенного накопления эмпирического опыта.

Этот процесс формирования взаимных представлений о приемлемом/неприемлемом поведении в ходе постоянной вовлечённости получил название *негласных переговоров* (от англ. – «*tacit bargaining*»).

Так, в документе «Достижение и поддержание превосходства в киберпространстве» процесс негласных переговоров раскрывается следующим образом: «Благодаря постоянным действиям и более эффективной конкуренции ниже уровня вооружённого конфликта мы можем [...] *прояснять различие между приемлемым и неприемлемым поведением в киберпространстве*»[96]. В руководстве утверждается, что «операции США в киберпространстве могут внести позитивный вклад в дипломатическую мощь [...] *подавая противнику скрытые сообщения*»[97].

Данный подход к формированию приемлемых норм нашёл отражение и в Отчёте комиссии по киберпространству «Солярий», в котором сказано, что посредством постоянной вовлечённости подразумевается осуществление упреждающей защиты и создание стратегических издержек для противников не только с целью сдержать будущие кибератаки противника, но и «укрепить предпочтительные нормы поведения в киберпространстве»[98].

Ричард Харкнетт и Майкл Фишеркеллер утверждают, что «чем интенсивней осуществляется конкурентное взаимодействие в пространстве согласованной конкуренции, тем больше ясности появится относительно разграничения незаконных или законных кибероперaций, а также относительно того, что находится в рамках или за рамками правил согласованной конкуренции»[99].

Нынешняя стратегическая мысль США предполагает, что правила поведения в кибепространстве между конкурирующими странами могут выработаться негласно за счет постепенного накопления эмпирического опыта и представлений о приемлемом и неприемлемом поведении

[95] Achieve and Maintain Cyberspace Superiority... P. 6; Fischerkeller M. P., Harknett R. J. Deterrence is Not a Credible... P. 381; Fischerkeller M. P., Harknett R. J. Persistent Engagement, Agreed Competition... P. 23; Fischerkeller M. P., Harknett R. J. Persistent Engagement and Tacit Bargaining...; Fischerkeller M. P., Harknett R. J. What Is Agreed...; Miller J. N., Pollard N. A. Persistent Engagement, Agreed Competition and Deterrence in Cyberspace [Electronic resource] / Lawfare. Washington, DC, 2019. Mode of access: https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace (date of access: 20.08.2020).
[96] Achieve and Maintain Cyberspace Superiority... P. 6.
[97] Achieve and Maintain Cyberspace Superiority... P. 4.
[98] The United States of America Cyberspace Solarium Commission. P. 24.
[99] Fischerkeller M. P., Harknett R. J. Persistent Engagement, Agreed Competition... P. 16.

В отличие от России, которая пытается формировать универсальные правила приемлемого поведения в киберпространстве на основе гласного и официального переговорного процесса в рамках ООН, Соединённые Штаты и их союзники будут «идентифицировать стратегический процесс, с помощью которого они могут разработать “modus vivendi”, не достигающий уровня вооружённого конфликта, в киберстратегическом конкурентном пространстве с теми, кто либо не может, либо не будет вести публичные переговоры, или же в случае прихода к соглашению, но в котором отсутствует взаимное доверие друг к другу»[100].

Более того, Майкл Фишеркеллер и Ричард Харкнетт идут ещё дальше, заявляя, что если Соединённые Штаты хотят активно «разрабатывать международные нормы для киберпространства, то они могут сделать это только *посредством активных кибероперации, которые начинают формировать параметры приемлемого поведения [...] разработка международных норм требует постоянной кибер-вовлечённости, а не оперативных ограничений [...]*»[101]. По их мнению, выработанные в ходе таких негласных переговоров договорённости впоследствии могут стать официальными международными соглашениями, а постоянная вовлечённость будет стимулировать сам процесс переговоров по вопросу обеспечения кибербезопасности[102].

Отсутствие юридически закреплённых правил поведения в киберпространстве на деле позволяет США действовать в рамках двойных стандартов, а также менять эти правила по своему усмотрению

Согласно стратегическому мышлению Вашингтона, такой подход приведёт к большей стабильности в киберпространстве, а не росту эскалации[103], так как негласные переговоры для формирования приемлемого поведения в киберпространстве – это процесс, который структурно согласован с уникальными особенностями киберпространства, такими как взаимосвязанность и постоянный контакт, и поддерживается стратегической средой самого киберпространства[104].

В то же время некоторые исследователи указывают на ряд очевидных недостатков стратегии постоянной вовлечённости с точки зрения формирования ею приемлемых правил поведения. Так, старший научный сотрудник Центра исследований безопасности Макс Смитс предупреждает, что при отсутствии юридически закреплённых правил поведения определённые действия в киберпространстве сегодня могут быть приемлемыми для одного субъекта, а завтра вдруг оказаться недопустимыми и повлечь за собой ответные меры[105]. Он также говорит, что имеют место быть и двойные стандарты, при которых какой-либо субъект считает оправданным осуществлять определённые кибероперации в отношении других, но неприемлемым в отношении себя[106]. Например, по словам Джейсона Хили, США сами установили нормы кибершпионажа, которые затем посчитали для себя недопустимыми[107].

Здесь важно не забывать и о том, что одна и та же кибе-

[100] Fischerkeller M. P., Harknett R. J. Persistent Engagement and Tacit Bargaining...
[101] Fischerkeller M. P., Harknett R. J. Deterrence is Not a Credible... P. 382.
[102] Fischerkeller M. P., Harknett R. J. Persistent Engagement and Tacit Bargaining...
[103] Fischerkeller M. P., Harknett R. J. Persistent Engagement and Tacit Bargaining...
[104] Fischerkeller M. P., Harknett R. J. Deterrence is Not a Credible... P. 381; Fischerkeller M. P., Harknett R. J. Persistent Engagement and Tacit Bargaining...
[105] Smeets M. There Are Too Many Red Lines in Cyberspace [Electronic resource] / Lawfare. Washington, DC, 2019. Mode of access: https://www.lawfareblog.com/there-are-too-many-red-lines-cyberspace (date of access: 22.08.2020).
[106] Smeets M. Cyber Command’s Strategy Risks Friction With Allies [Electronic resource] / Lawfare. Washing-ton, DC, 2019. Mode of access: https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies (date of access: 22.08.2020).
[107] Healey J. The implications of persistent...

роперация может иметь совершенно разные последствия для тех или иных государств в связи с их неравной степенью киберзависимости. Соединённые Штаты должны учитывать, что кибероперация в рамках постоянной вовлечённости, приемлемая для одного государства, может быть абсолютно неприемлемой для другого.

На данный момент так называемая «эскалационная лестница» применительно к киберпространству плохо изучена, поэтому тот или иной шаг в киберпространстве может быть нормальным для одного участника потенциального конфликта, и совершенно неприемлемым – для другого[108].

Более того, Джейсон Хили заявляет, что такая «риторика создает дополнительную неопределённость в отношении намерений США [...] Даже если противники идентифицируют и поймут сигналы США, *они не могут быть уверены в том, что возмездие прекратится, даже если их поведение будет соответствовать предпочтениям Соединённых Штатов*»[109].

В любом случае, сами американские эксперты отмечают, что на сегодняшний день процесс негласных переговоров всё ещё находится на стадии своего формирования и требует более детального изучения для определения допустимых типов эффектов[110].

НОВАЯ СТРАТЕГИЯ ПОСТОЯННОЙ ВОВЛЕЧЁННОСТИ И СОПУТСТВУЮЩИЕ РИСКИ

Однако, теоретически решая одну проблему, новый стратегический подход одновременно может повлечь за собой и определённые риски. В главном документе Киберкомандования США, декларирующем стратегию постоянной вовлечённости, делается *небольшая* (на 2/3 стр.) попытка проанализировать риски данного подхода. Всего в документе выделено 2 риска.

Первый риск – стратегия постоянной вовлечённости сосредотачивается на противодействии государствам, упуская из виду другие субъекты, действующие в киберпространстве, и по отношению к которым нужна другая стратегия[111].

Второй (и более важный на наш взгляд) риск – дипломатический. В «Достижениях» США выражают понимание того, что мировое сообщество критически отнесётся к применению Белым Домом данной стратегии и воспримет её как агрессивную и милитаризующую киберпространство[112].

Первый риск Киберкомандование планирует снизить путём улучшения кибероборонысетей Министерства обороны, а также путём обмена разведданными и оперативными данными с правоохранительными органами, органами национальной безопасности и разведывательным сообществом.

Снижение второго риска будет связано с убеждением общественности в необходимости принимаемых мер.

---

[108] Nye J. S. Deterrence and Dissuasion in Cyberspace. P. 70; Nye J. S. Nuclear Lessons for Cyber Security. P. 26.

[109] Healey J., Caudill S. Success of Persistent Engagement in Cyberspace [Electronic resource] / Strategic Studies Quarterly. 2020. Vol. 14, No. 1. P. 11. Mode of access: https://www.jstor.org/stable/26891881?seq=1#metadata_info_tab_contents (date of access: 03.09.2020).

[110] Fischerkeller M. P., Harknett R. J. Persistent Engagement, Agreed Competition... P. 23; Fischerkeller M. P., Harknett R. J. What Is Agreed...

[111] Achieve and Maintain Cyberspace Superiority... P. 10.

[112] Achieve and Maintain Cyberspace Superiority... P. 10.

Стратегия постоянной вовлеченности не учитывает глобальный и геополитический контекст, может представлять собой акт агрессии и привести к реальному военному ответу

Однако, некоторые американские эксперты, проанализировав стратегию постоянной вовлечённости, выделили гораздо больше рисков, сопутствующих осуществлению нового подхода, которые могут привести к непреднамеренной эскалации[113].

> I. Те или иные кибероперации, осуществляемые в рамках постоянной вовлечённости, могут представлять собой акт агрессии и привести к несопоставимым со стратегической конкуренцией последствиям, и вследствие этого повлечь за собой применение традиционных «физических» ответных мер. В этом случае конфликт может «выйти» за пределы противоборства в киберпространстве и перейти в традиционную область военных действий[114].
> II. Стратегия постоянной вовлечённости в киберпространстве фокусируется лишь собственно на киберпространстве и рассматривается в «вакууме», не учитывая глобальный стратегический и геополитический контекст, в то время как конфликт опять же может перерасти в традиционное противоборство[115].
> III. Вместо того, чтобы отступить под давлением наложенных Соединёнными Штатами стратегических издержек, противник может попытаться преодолеть американскую упреждающую защиту[116]. Это более верно в условиях того, что различные стороны стремятся к достижению превосходства, а не к сдержанности и стабильности.

В экспертном сообществе США пока не сложилось единое мнение относительно политики постоянной вовлеченности: одни эксперты считают ее универсальной, а другие – не имеющей долгосрочных стратегических преимуществ

В то время, как одними экспертами постоянная вовлечённость рассматривается в качестве универсального подхода, учитывающего уникальные характеристики киберпространства и реалии сегодняшнего дня, другие заявляют, что «не может быть универсального решения, когда речь заходит о стратегическом постоянстве в кибердомене»[117]. Например, старший научный сотрудник Лаборатории прикладной физики Университета Джона Хопкинса Джеймс Миллер и адъюнкт-профессор Школы международных и общественных отношений Колумбийского университета Нил Поллард вообще сомневаются в том, приведет ли постоянная вовлечённость к долгосрочным стратегическим преимуществам[118]. Джейсон Хили призывает более детально изучить стратегию постоянной вовлечённости, так как её последствия могут быть абсолютно непредсказуемыми. Более того, он открыто заявляет, что при стратегической конкуренции в киберпространстве ошибки неизбежны – как со стороны самих Соединённых Штатов, так и их противников, и рано или поздно одна из сторон соперничества зайдёт слишком далеко[119], что не может не настораживать.

Политика относительно принятия новой стратегии на на-

[113] Lin H., Smeets M. What Is Absent From the U.S. Cyber Command 'Vision' [Electronic resource] / Lawfare. Washington, DC, 2018. Mode of access: https://www.lawfareblog.com/what-absent-us-cyber-command-vision (date of access: 23.08.2020).
[114] Healey J. The implications of persistent...; Kollars N., Schneider J. Defending Forward: the 2018 Cyber Strate-gy is Here [Electronic resource] / War on the Rocks. Washington, DC, 2018. Mode of access: https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/ (date of access: 23.08.2020).; Miller J. N., Pollard N. A. Persistent Engagement...
[115] Kollars N., Schneider J. Defending Forward...; Miller J. N., Pollard N. A. Persistent Engagement...
[116] Healey J. The implications of persistent...
[117] Lin H., Smeets M. What Is Absent...
[118] Miller J. N., Pollard N. A. Persistent Engagement...
[119] Healey J. The implications of persistent...

стоящий момент критикуется по той причине, что в новых стратегических документах США не делается адекватных попыток изучить возможную эскалацию, которая может возникнуть вследствие применения постоянной вовлечённости[120]. Так или иначе, но исследователи утверждают, что необходимо далее изучать, какие типы целей или эффектов могу привести к эскалации, а также проанализировать ценность других различных подходов к обеспечению кибербезопасности[121].

Центр кибероперацій в Форт-Гордон, США

Источник: www.army.mil

СТРАТЕГИЯ В ДЕЙСТВИИ. АНАЛИЗ ПРИМЕРОВ ПРИМЕНЕНИЯ ПОСТОЯННОЙ ВОВЛЕЧЁННОСТИ

Как предполагается, впервые стратегия постоянной вовлечённости была применена на практике в 2018 г., когда, согласно заявлению Киберкомандования США, им удалось предотвратить «очередное» предполагаемое вмешательство России в «промежуточные выборы» США, проходившие 6 ноября 2018 г., и вследствие проведённой кибероперации заблокировать доступ в интернет так называемой «Фабрике троллей» (или «Агентству интернет-исследований»)[122], деятельность которой, по мнению Соединённых Штатов, направлена на подрыв процесса демократических выборов в США[123].

По словам американских высокопоставленных лиц, данная кибероперация – всего лишь часть общей *постоянной киберкомпании* против «Российского вмешательства»[124]. Также, эта операция стала первой пробой пера предоставленных Киберкомандованию США наступательных полномочий в связи с принятием президентского меморандума о национальной безопасности №13 и изменением «Национального закона о государственной обороне».

Другим примером реализации стратегии постоянной вовлечённости может служить необъявленное и идущее уже долгое время киберпротивостояние между Соединёнными Штатами и Ираном, в котором взаимные кибероперации происходят

[120] Buchanan B. The Implications of Defending Forward in the New Pentagon Cyber Strategy [Electronic re-source] / Council on Foreign Relations. New York, NY, 2018. Mode of access: https://www.cfr.org/blog/cyber-week-review-september-21-2018 (date of access: 25.08.2020); Lin H., Smeets M. What Is Absent...

[121] Healey J. The implications of persistent...; Kollars N., Schneider J. Defending Forward...; Lin H., Smeets M. What Is Absent...

[122] Statement of General Paul M. Nakasone Commander United States Cyber Command Before the Senate Com-mittee on Armed Services [Electronic resource] / Senate Committee on Armed Services. New York, NY, 2019. P. 4. Mode of access: https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf (date of access: 12.07.2020); Nakashima E. U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms [Electronic resource] / The Washington Post. Washington, DC, 2019. Mode of access: https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html (date of access: 12.07.2020); Barnes J. E. Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections [Electronic resource] / The New York Times. New York, NY, 2019. Mode of access: https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html (date of access: 12.07.2020); Schneider J. G. Persistent Engagement...

[123] Именно «Агентство интернет-исследований» было обвинено Министерством юстиции США во вмеша-тельстве в выборы американского президента в 2016-м г. по результатам расследований спецпрокурора США Роберта Мюллера.

[124] Barnes J. E. Cyber Command Operation...; Nakashima E. U.S. Cyber Command operation...

на постоянной основе в так называемой «серой зоне» международного права, и, что самое главное – эти кибероперации не достигают уровня вооружённого конфликта[125]. Так, в рамках американо-иранского конфликта Соединёнными Штатами были осуществлены кибератаки на компьютерную сеть Корпуса Стражей Исламской революции, которые на некоторое время парализовали работу систем с целью сорвать возможность Ирана атаковать иностранные танкеры в Персидском заливе[126].

Два этих случая действительно являются яркими примерами операций, осуществлённых Соединёнными Штатами в рамках стратегии постоянной вовлечённости. Об этом свидетельствуют следующие факторы: 1) они предусматривают постоянный контакт со Стороны США; 2) они не достигают уровня вооружённого конфликта; 3) они создают тактические препятствия для «противников» США; 4) они явно являются «упреждающими».

НОВАЯ СТРАТЕГИЯ ПОСТОЯННОЙ ВОВЛЕЧЁННОСТИ США И ДАЛЬНЕЙШИЕ ВЗАИМООТНОШЕНИЯ МЕЖДУ РОССИЕЙ И СОЕДИНЁННЫМИ ШТАТАМИ ПО ВОПРОСУ КИБЕРБЕЗОПАСНОСТИ

Итак, концептуальные и институциональные изменения в политике кибербезопасности США носят проактивный характер и явно направлены на то, чтобы предоставить большую свободу действий Соединённым Штатам в киберпространстве с целью достижения ими стратегического превосходства.

Исходя из всех этих изменений можно ли предполагать, что Соединённые Штаты в дальнейшем не намерены вести дипломатический диалог (с Россией, в частности), придерживаться международного сотрудничества как меры противодействия киберугрозам и продвигать какие-либо международные нормы поведения в киберпространстве, тем самым развязывая себе руки для развития более широкого противостояния во всех областях, в которых получает распространение стратегическая конкуренция великих держав?

Выше уже было рассмотрено то, как США сначала заявили о вступлении в долгосрочную стратегическую конкуренцию в «реальном» мире, а затем и в киберпространстве. Например, в «Стратегии национальной безопасности США» 2017 г. утверждается, что политика Соединённых Штатов, согласно которой «взаимодействие с конкурентами и включение их в процесс международного сотрудничества с целью превращения их в добросовестных игроков и надёжных партнеров», оказалась ошибочной[127]. А в документе «Достижение и поддержание превосходства в киберпространстве» напрямую сообщается, что, даже если в применении стратегии постоянной вовлечённости международное сообщество увидит попытки США милитаризовать киберпространство,

[125] Barnes J. E., Gibbons-Neff T. U.S. Carried Out Cyberattacks on Iran [Electronic resource] / The New York Times. New York, NY, 2019. Mode of access: https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html (date of access: 20.02.2021).

[126] Barnes J. E., Gibbons-Neff T. U.S. Carried Out...; Barnes J. E. U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say [Electronic resource] / The New York Times. New York, NY, 2019. Mode of access: https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html (date of access: 20.02.2021); US 'launched cyber-attack on Iran weapons systems' [Electronic resource] / BBC News. 2020. Mode of access: https://www.bbc.com/news/world-us-canada-48735097 (date of access: 20.02.2021).

[127] National Security Strategy of the United States of America. P. 3, 27.

Киберкомандование США «не собирается извиняться за защиту интересов США в соответствии с указанием президента [...] в области, уже военизированной нашими противниками»[128]. Поэтому, согласно Вашингтону, он и вступает в стратегическую конкуренцию, приняв новую стратегию постоянной вовлечённости.

В целом, согласно описанным документам – «Киберстратегии Министерства обороны США» 2018 г., «Национальной киберстратегии Соединённых Штатов Америки» 2018 г., и рекомендательному Отчёту комиссии по киберпространству «Солярий» – международное сотрудничество и нормотворчество также являются важными механизмами предотвращения киберугроз. Так, в «Киберстратегии Министерства обороны США» утверждается, что «Министерство будет укреплять добровольные нормы ответственного поведения государств в киберпространстве в мирное время»[129]. Об этом же говорится и в «Национальной киберстратегии» США, согласно которой «Соединённые Штаты будут продвигать нормы ответственного поведения государства в киберпространстве, основанные на международном праве»[130]. В том же Отчёте комиссии по киберпространству «Солярий» продвижение международных норм является первым уровнем многоуровневого сдерживания, в рамках которого «стратегия призывает к формированию ответственного поведения и поощрению сдержанности в киберпространстве путём усиления норм и невоенных инструментов»[131]. Согласно Отчёту, «система норм, созданная на основе международного взаимодействия и сотрудничества, будет способствовать ответственному поведению государств и со временем удерживать противников от использования кибероперации для подрыва интересов любой страны»[132]. В таком случае непонятно, почему США не прибегают к использованию этих методов, а предпочитают в одностороннем порядке сразу же осуществлять упреждающие кибероперации, как в случае с предполагаемой «Фабрикой троллей».

Однако, в том же Отчёте комиссии по киберпространству «Солярий» также сообщается, что Соединённые Штаты будут «коллективно разрабатывать и внедрять кибернормы» лишь совестно с американскими «партнёрами и союзниками», и эти нормы будут основаны на их «общих интересах и ценностях»[133]. Более того, в «Национальной киберстратегии Соединённых Штатов Америки» 2018 г. было заявлено о планах реализовать так называемую «Инициативу киберсдерживания», в рамках которой предполагалось создание коалиции государств-*единомышленников* для «координации и поддержки ответных действий друг друга на серьезные злонамеренные киберинциденты» – то есть для более эффективного реагирования на кибератаки и наложения последствий на противников США[134]. Документ Госдепартамента США «О международной безопасности в киберпространстве [...]» 2020 г. подтверждает приверженность реализации данной инициативы киберсдежривания с целью создания «общего потенциала для быстрого наложения последствий» и «гибкой модели для организации совместного реагирования на серьезные киберинциденты»[135].

[128] Achieve and Maintain Cyberspace Superiority... P. 10.
[129] The Department Of Defense Cyber Strategy 2018... P. 5.
[130] National Cyber Strategy of the United States of America. P. 20.
[131] The United States of America Cyberspace Solarium Commission. P. 3.
[132] The United States of America Cyberspace Solarium Commission. P. 3.
[133] The United States of America Cyberspace Solarium Commission. P. 24.
[134] National Cyber Strategy of the United States of America. P. 21.
[135] Ford. C. A. International Security in Cyberspace... P. 6.

Как видно из этих примеров, США собираются развивать сотрудничество в сфере обеспечения кибербезопасности лишь с союзниками. Значит ли это, что Соединённые Штаты не собираются договариваться с другими государствами, учитывать их ценности, и не будут идти на компромисс?

Можно сделать вывод, что, принимая на вооружение стратегию постоянной вовлечённости, Вашингтон в то же время надеется оставить себе поле для манёвра и дипломатического диалога со своими стратегическими конкурентами.

Очевидно, что главной целью новой Киберстратегии США является не сохранение стабильности и доверия, а достижение собственного превосходства

Это удобная позиция для США, однако необходимо *помнить, что односторонние кибероперации в рамках постоянной вовлечённости никак не способствуют эффективному сотрудничеству и укреплению взаимного доверия.*

Проанализированные изменения в концепции кибербезопасности США могут свидетельствовать о том, что США не готовы дожидаться какой-либо позитивной динамики в переговорах по вопросу обеспечения международной кибербезопасности, и уже сейчас явно превращают киберпространство в операционную область и милитаризируют его. Вне киберконтекста о расширении стратегической конкуренции говорилось ещё в «Стратегии национальной обороны» 2018 г., согласно которой Соединённые Штаты и далее «будут расширять конкурентное пространство, перехватывая инициативу»[136]. Однако в своей совместной статье в Foreign Affairs глава Киберкомандования США генерал Пол Накасоне, и руководитель проекта по кибербезопасности Белфер-Центра в Гарвардской школе Кеннеди Майкл Сулмейер утверждают, что «это расширение должно было затронуть и киберпространство»[137].

Таким образом, становится ясно, что посредством стратегии постоянной вовлечённости усилия США направлены не на поиск компромисса, укрепление доверия и сохранение стабильности в киберпространстве, а прежде всего на достижение собственного превосходства в киберпространстве и завладение инициативой.

Здесь необходимо отметить, что в ближне- и среднесрочной перспективе не стоит ожидать, что США откажутся от стратегии постоянной вовлечённости и участия в стратегической конкуренции. Новый глава Белого Дома Джо Байден уже выразил желание продолжить эту политику, однако с условием её должного анализа, и, возможно, пересмотра, так как стратегия постоянной вовлечённости «может иметь непредвиденные последствия, выходящие за рамки киберпространства», о чём он заявил в интервью газете The New York Times, когда ещё не был избран[138].

Сам Байден поддержал несколько инициатив в области кибербезопасности администрации Трампа, в том числе Президентский меморандум о национальной безопасности № 13 «О наступательных кибероперациях» (NSPM 13), который отменил директиву

[136] Summary of the 2018 National Defense Strategy of the United States of America... P. 4, 5.
[137] Nakasone P.M., Sulmeyer M. How to Compete in Cyberspace.
[138] Cyber Policy [Electronic resource] / The New York Times. New York, NY, 2019. Mode of access: https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html (date of access: 13.02.2021).

президента США № 20 (PPD-20)[139]. Этот указ, как уже было упомянуто, дал военным больше полномочий для преследования противников США в киберпространстве. Байден также пообещал «наложить существенные и долгосрочные издержки» на любую страну, которая вмешивается в выборы США, в отличие от Трампа, который данную повестку вмешательства старался игнорировать. Более того, новая администрация Белого дома примет во внимание рекомендации, изложенные в Отчёте комиссии по киберпространству «Солярий», которые не получили поддержки при администрации Дональда Трампа. Это может означать, что постоянная вовлечённость будет принята в качестве элемента «многоуровневого сдерживания», описанного в Отчёте.

Свидетельством продолжения принятого Дональдом Трампом курса может служить опубликованное в январе 2021 г. «Руководство для новой администрации Байдена: Белая книга Комиссии по киберпространству “Солярий” № 5», представляющее из себя пакет рекомендаций по обеспечению кибербезопасности для новой администрации Белого дома. Этот документ определяет возможные действия и устанавливает приоритеты на ближайшие месяцы и годы. Так, концепция упреждающей защиты, которая реализовывается посредством стратегии постоянной вовлечённости, упоминается в документе 9 раз. Однако, в документе заявляется, что несмотря на полномочия по активному осуществлению кибероперации вне национальных американских сетей, которые были предоставлены Киберкомандованию, стратегия, ориентированная на превентивное предотвращение кибератак ещё до их осуществления, остаётся одной из белых пятен киберполитики администрации Дональда Трампа, поэтому новая «администрация Байдена-Харрис должна пересмотреть и доработать концепцию превентивной защиты и предоставления полномочий для осуществления наступательных кибероперации, тем самым обеспечив адекватную оценку рисков и выгод при сохранении необходимой ориентации на быстрые действия»[140].

Масло в огонь подлила и киберкампания Sunbirst, о которой стало известно в середине декабря 2020 г., и которая, по оценкам американских экспертов, стала самой беспрецедентной и широкомасштабной за последние пять лет[141]. В рамках этой киберкампании хакеры при поддержке иностранного правительства взломали системы государственных ведомств США – Министерства финансов, Национального управления по телекоммуникациям и информации Министерства торговли, Министерства внутренней безопасности, Министерства энергетики, Национального управления ядерной безопасности США, лаборатории в Лос-Аламосе (занимается секретными разработками по ядерному

[139] Cyber Policy...; Geller E. Biden prepping to ramp up U.S. cyber defenses — while keeping some Trump poli-cies [Electronic resource] / Politico. Arlington, Virginia,2020. Mode of access: https://www.politico.com/news/2020/08/20/joe-biden-cyber-defenses-399530 (date of access: 13.02.2021).

[140] Cyberspace Solarium Commission White Paper #5: Transition Book for the Incoming Biden Administration [Electronic resource] / U.S. Cyberspace Solarium Commission. Washington, DC, 2021. P. 11. URL: https://www.solarium.gov/public-communications/transition-book (date of access: 25.02.2021).

[141] Nakashima E., Timberg C. Russian government hackers are behind a broad espionage campaign that has com-promised U.S. agencies, including Treasury and Commerce [Electronic resource] / The Washington Post. Washington, DC, 2020. Mode of access : https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html (date of access: 28.02.2021).

оружию), Госдепартамента, федерального правительства и даже Пентагона. Взлому также подверглись и большинство крупнейших частных компаний из знаменитого списка Fortune 500, в том числе Microsoft. Американские СМИ со ссылкой на источники и спецслужбы США, среди которых ФБР, АНБ и Управление директора Национальной разведки, данное масштабное кибервмешательство вновь приписали России[142]. Американские эксперты предполагают, что за данной киберкампанией стоит хакерская группировка Cozy Bear (кодовое название – APT29), которая якобы работает на Службу внешней разведки РФ.

Очень интересно то, что сведения об этой кибератаке были обнародованы как раз в тот момент, когда коллегия выборщиков признала победу Джо Байдена на выборах. Обнаруженная как раз кстати – к признанию победы Джо Байдена – и вновь приписанная России, она нарочито напоминает новому президенту Соединённых Штатов о «российской угрозе», которую теперь уже нельзя игнорировать. Можно предположить, что новые вышеописанные обвинения в адрес России могут являться целенаправленным вбросом, призванным подстегнуть Байдена к проведению в отношении России более активных действий, направленных на предотвращение якобы её злонамеренной активности в киберпространстве.

Крайне важно, что Джо Байден во время предвыборной кампании неоднократно в негативном ключе отзывался о России. 21 июля 2020 г. на своей странице в социальной сети Medium он сделал заявление, что в случае избрания его президентом он будет «рассматривать иностранное вмешательство в [американские. – С.А.] выборы как акт соперничества, который существенно влияет на отношения между Соединёнными Штатами и правительством вмешивающейся страны [...] Если какая-либо иностранная держава опрометчиво решит вмешаться в нашу демократию, я без колебаний отвечу как президент [...]»[143]. Важно, что в данном заявлении он неоднократно обращает внимание на Россию. Похожие заявления он делал во время прямой линии на телеканале CNN 17 сентября 2020 г., а также во время вторых дебатов с Д. Трампом 22 октября 2020 г.[144]

А теперь ещё внимание Байдена привлекла и киберкампания Sunbirst, после которой он сделал новые заявления. Так, 22 декабря 2020 г. во время пресс-конференции Джо Байден, основываясь на утверждениях государственного секретаря Майка Помпео и генерального прокурора Уильяма Барра, возложил вину за данные кибератаки на Россию, заявив, что новая администрация Белого Дома в обязательном порядке предпримет ответные меры в отношении предполагаемого агрессора[145].

---

[142] Bing C. Suspected Russian hackers [Electronic resource] / Reuters. 2020. Mode of access: https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive/exclusive-hackers-spied-on-u-s-treasury-emails-for-a-foreign-government-sources-idUSKBN28N0PG (date of access: 27.02.2021).

[143] Biden J. My Statement on Foreign Interference in U.S. Elections [Electronic resource] / Medium. San Francis-co, CA, 2020. Mode of access: https://medium.com/@JoeBiden/my-statement-on-foreign-interference-in-u-s-elections-8b42b4444eb6 (date of access: 27.02.2021).

[144] The Latest: Biden Says Russia Will Pay for Election Meddling [Electronic resource] / U.S. News. Washington, DC, 2020.Mode of access: https://www.usnews.com/news/politics/articles/2020-09-17/the-latest-biden-says-campaign-will-focus-on-early-voting (date of access: 27.02.2021); Campaign 2020. Trump-Biden Second Debate [Electronic resource] / C.-Span. Washington, DC, 2020. URL: https://www.c-span.org/video/?475796-1/trump-biden-debate&live (date of access: 26.02.2021).

[145] Biden says huge data breach poses 'grave risk' to U.S., promises response [Electronic

Однако «ветер дует» не только от самого Байдена, но и от его «старших советников»-демократов. Дело в том, что после победы кандидата от республиканской партии Дональда Трампа на выборах 8 ноября 2016 г., чему, как полагают в США, поспособствовало «российское вмешательство», демократы в лице «старших советников» Байдена на четыре года оказались отстранёнными от власти[146]. Возможно, движимые желанием взять реванш, они будут подталкивать нового главу Белого дома к осуществлению более настойчивых шагов в отношении России за приписываемое ей вмешательство в выборы 2016 г. Сам Дональд Трамп полностью отрицал какую-либо помощь якобы со стороны российских спецслужб.

Как представляется, уверенность в причастности России к Sunbirst в очередной раз убедила Джо Байдена в необходимости наказать Москву за все приписываемые ей кибератаки, которые на этот раз приняли беспрецедентные масштабы. Так, предполагаемые ответные меры активно обсуждаются ещё с декабря 2020 г. (когда сам Байден ещё не вступил в должность)[147]. Среди обсуждаемых мер – санкции и ответный взлом российских систем[148].

Здесь важно обратить внимание на заявление нового руководителя аппарата сотрудников Белого дома Рона Клайна, согласно которому необходимо «снизить способность иностранных субъектов повторить такого рода атаку или, что еще хуже, участвовать в еще более опасных атаках»[149]. На наш взгляд, под формулировкой «снижение способности “иностранных субъектов”» вполне можно понимать применение постоянной вовлечённости. Похоже, что киберкампания Sunbirst убедила руководство Соединённых Штатов в необходимости продолжать проведение и совершенствовать стратегию постоянной вовлечённости. Например, Ричард Харкнетт выразил надежду, что после Sunbirst постоянная вовлечённость станет основой политики обеспечения кибербезопасности США, так как данная кибератака явно обнажила факт того, что в киберпространстве сегодня получает распространения стратегическая конкуренция[150].

Сегодня США явно демонстрируют, что они не готовы договариваться с Россией по вопросу урегулирования накопившихся между двумя странами проблем в сфере киберполитики.

resource] / Reuters. 2020. Mode of access: https://www.reuters.com/article/idUSKBN28W2G8 (date of access: 27.02.2021).

[146] Джо Байден был вице-президентом США в администрации демократа Барака Обамы, но покинул этот пост после победы в 2016 г. кандидата от Республиканской партии Дональда Трампа.

[147] Satter R. Biden chief of staff says hack response will go beyond ‘just sanctions’ [Electronic resource] / Reu-ters. 2020. Mode of access: https://www.reuters.com/article/idUSKBN28U0IK (date of access: 27.02.2021).

[148] Hunnicutt T., Lawder D., Psaledakis D. Biden’s options for Russian hacking punishment: sanctions, cyber re-taliation [Electronic resource] / Reuters. 2020. Mode of access: https://www.reuters.com/article/idUSKBN28U0DV (date of access: 28.02.2021).

[149] В администрации Байдена заявили, что ответ на кибератаки не ограничится санкциями // ТАСС : сайт. 2020. URL:: https://tass.ru/mezhdunarodnaya-panorama/10307005 (дата обращения: 28.02.2021).

[150] Harknett R. J. SolarWinds: The Need for Persistent Engagement [Electronic resource] / Lawfare. Washington, DC, 2020. Mode of access: https://www.lawfareblog.com/solarwinds-need-persistent-engagement (date of access: 23.02.2021).

Так, последняя Российская инициатива – «Комплексная программа мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности»[151], предложенная президентом России В.В. Путиным 25 сентября 2020 г. – была полностью отвергнута Вашингтоном несмотря на то, что, на наш взгляд, в данной «комплексной программе» сформулированы позитивные и вполне жизнеспособные предложения американской стороне[152]. Более того, как уже было сказано, 20 октября 2020 г. – т.е. уже после выдвинутых В.В. Путиным предложений – Госдепартаментом США был опубликован документ «О международной безопасности в киберпространстве», в котором говорится о конкуренции в киберпространстве с Россией и который имеет ярко-выраженную и резко-антироссийскую риторику, что говорит об отсутствии у Белого дома желания в ближайшей перспективе договариваться с нами.

Вашингтон глубоко убеждён в том, что Москва активно осуществляет кибератаки в отношении американского демократического процесса, американских систем и инфраструктуры, и что такие кибератаки продолжатся и в будущем. Именно из-за этого как вышеуказанные предложения, так и те, которые могли бы быть выдвинуты в ближайшем будущем, воспринимались и будут восприниматься в Вашингтоне как лицемерие российской стороны. США видят в России непримиримого соперника, который продолжит осуществлять кибератаки, но при этом всячески старается снять с себя все возможные подозрения.

Похоже, что и Россия уже потеряла надежду на нормализацию конструктивного взаимодействия с США по вопросу киберповестки. В своём интервью от 23 декабря 2020 г. заместитель министра иностранных дел РФ Сергей Рябков по поводу выдвигаемых в сторону России обвинений в кибератаках и возможности восстановления диалога касательно поведения в киберпространстве, заявил следующее – «что бы мы ни делали, какие бы мы ни давали опровержения, сколько бы мы ни употребляли каких-то риторических приемов, чтобы это опровергнуть, ситуация от этого не изменится. Поэтому я не вижу предмета для дискуссий на эту тему»[153]. Он заявил, что Россия по отношению к США должна переходить к двухтрековому подходу: 1) тотальное сдерживание США по всем направлениям, «поскольку политика США глубоко враждебна по отношению к России»; 2) выборочный диалог и вовлечение США только по тем сюжетам, которые интересны Москве[154].

Таким образом, кризис, сложившейся между Москвой и Вашингтоном в киберсфере, скорее всего, будет усугубляться. По этому поводу Ричард Сокольский и Юджин Румер в своем докладе «Российско-американские отношения в 2030 году» дают очень неутешительный прогноз. Согласно им, «*впереди у России и США много лет ничем не сдерживаемого соревнования в киберсфере [...]*

[151] Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности // Президент России : сайт. 2020. URL: http://www.kremlin.ru/events/president/news/64086 (дата обращения: 22.10.2020).

[152] Черненко Е. «Не более чем циничная и дешевая пропаганда»: США отвергли предложение Владимира Путина по кибербезопасности // Коммерсантъ : сайт. 2020. URL: https://www.kommersant.ru/doc/4539391#id1963636 (дата обращения: 24.10.2020).

[153] Сергей Рябков: Россия в отношениях с США должна перейти к политике сдерживания и избирательного диалога : интервью // Интерфакс : сайт. 2020. URL: https://www.interfax.ru/interview/742593 (дата обра-щения: 28.02.2021).

[154] Сергей Рябков: Россия в отношениях с США...

Условия для выработки норм поведения, контроля или (что вероятнее) мер повышения доверия [...] возникнут нескоро»[155]. Аналогичного мнения придерживается и консультант ПИР-Центра, старший эксперт Центра перспективных управленческих решений Олег Шакиров, который утверждает, что в «предстоящее десятилетие политические разногласия [...] помешают достижению значительного прогресса в переговорном процессе по безопасности киберпространства на международном уровне»[156].

Что же делать России в данных условиях?

В некоторых аспектах России будет крайне трудно конкурировать с Соединёнными Штатами в силу объективного технологического отставания. Несмотря на то, что США подозревают Россию во всех своих «кибербедах», они не сомневаются в своём технологическом превосходстве. Зачем Вашингтону договариваться с более слабым чем он сам конкурентом?

Здесь уместно будет привести аналогию с обладанием ядерным оружием. Равноправный диалог и договорённости между СССР и США стали возможны только тогда, когда обе страны достигли паритета относительно ядерной мощи. России следует работать в этом направлении, стимулировать развитие отечественных технологий и сокращать технологический разрыв – это может стимулировать Вашингтон начать диалог по вопросу взаимодействия в киберпространстве. Однако представляется маловероятным, что в ближайшем будущем Россия достигнет значительного технологического паритета с Соединёнными Штатами. Например, согласно рейтингу сайта Top-500, США имеет 113 суперкомпьютеров, занимая 2 место. У России – всего 2 суперкомпьютера и 21 место в рейтинге. Показательно, что абсолютным лидером по количеству суперкомпьютеров является Китай – у него в арсенале 214 суперкомпьютеров[157].

Таким образом, в этом плане на роль явного конкурента США претендует Китай. Возможно, именно между этими двумя государствами развернётся наиболее масштабная стратегическая конкуренция в киберсфере[158]. Согласно «Докладу о цифровой экономике 2019», подготовленному экспертами Конференции ООН по торговле и развитию (ЮНКТАД), именно США и Китай сегодня занимают лидирующие позиции в развитии цифровой экономики[159]. Согласно прогнозу McKinsey в докладе «Цифровая Россия:

На данный момент из-за объективного технического отставания Россия не сможет стать равноправным конкурентом США в киберпространстве; России нужно развивать собственную технологическую базу для достижения паритета

[155] Sokolsky R., Rumer E. U.S.-Russian Relations in 2030 [Electronic resource] / Carnegie Endowment for Inter-national Peace. Washington, DC, 2020. P. 16. Mode of access: https://carnegieendowment.org/files/SokolskyRumer_US-Russia-2030_final1.pdf (date of access: 15.10.2020).

[156] Шакиров О. Будущее российско-американских отношений // Российский совет по международным де-лам : сайт. 2020. С. 7. URL: https://russiancouncil.ru/papers/Russia-USA-PolicyBrief31.pdf (дата обраще-ния: 15.10.2020)

[157] Данные приведены по состоянию на ноябрь 2020 г. Источник: List Statistics [Electronic resource] / Top-500. Mode of access: https://www.top500.org/statistics/list/ (date of access: 25.02.2021).

[158] Себекин С. А. Будущее международной системы информационной безопасности в условиях кризиса ар-хитектуры стратегической стабильности // Российский совет по международным делам : сайт. 2020. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/budushchee-mezhdunarodnoy-sistemy-informatsionnoy-bezopasnosti-v-usloviyakh-krizisa-arkhitektury-str/ (дата обра-щения: 28.02.2021).

[159] Доклад о цифровой экономике 2019. Создание стоимости и получения выгод: последствия для развива-ющихся стран : обзор // Конференция Организации Объединенных Наций по торговле и развитию обзор. ЮНКТАД : сайт. 2019. С. 3, 5. URL: https://unctad.org/system/files/official-document/der2019_overview_ru.pdf (дата обращения: 28.02.2021).

новая реальность», к 2025 г. доля цифровой экономики в ВВП США будет достигать 10.9%, а в ВВП Китая — 10%[160]. Это самые высокие показатели среди всех стран. Трудно представить, что конкуренция в этой сфере не стимулирует между ними также конкуренцию в киберпространстве и рост актов кибершпионажа.

России в таком случае стоит отойти от битвы двух «гигантов», одновременно пытаясь извлечь для себя выгоды из возможного американо-китайского киберпротивостояния, и стать арбитром в этом противостоянии, попутно пытаясь нарастить собственный кибероборонный потенциал.

Раз уж в ближайшем будущем между Москвой и Вашингтоном отсутствуют перспективы нормализации отношений в киберсфере, и с учётом взятия Соединёнными Штатами курса на стратегическую конкуренцию в киберпространстве, представляется возможным лишь переход к точечным мерам и таким же форматам взаимодействия, которые в большинстве своём будут носить односторонний характер (не считая сотрудничества с партнёрами).

Во-первых, можно в одностороннем порядке *установить пороги допустимых* масштабов и последствий от кибервторжения, *превышение которых повлечёт за собой осуществление определённых пропорциональных ответных мер разного уровня*.

Однако, установка лишь одного конкретного недопустимого порога масштабов и последствий может послужить сигналом того, что вплоть до него Россия (как государство-жертва) не будет реагировать, и, соответственно, побудить соперника намеренно совершать кибератаки, не пересекая его. Поэтому России необходимо рассмотреть ряд различных ответных мер чтобы использовать их против целого спектра различных угроз. Установка слишком низкого порогового значения означает необходимость реагирования на все атаки, что невозможно и бессмысленно. Установка же слишком высокого порогового значения даст понять противнику, что он может атаковать до заданного значения ущерба без последствий для себя. Поэтому порог реагирования должен быть «гибким» и включать множество вариантов возможных ответов разного уровня.

Также необходимо помнить, что в силу динамичной эволюции киберугроз сами кибервторжения невозможно ранжировать иерархически. Поэтому главным показателем того, необходимо ли реагировать и как реагировать, *служит* не сама кибератака и её мощь, *а произведенные эффекты и последствия от кибератаки*, так как их легко ранжировать. Важно дать понять потенциальному сопернику, что Россия будем руководствоваться именно этим принципом. Вследствие этого, важно чётко определить, какие атаки неприемлемы и являются актом агрессии, а какие являются незначительными издержками информационной эпохи.

Установка подобных порогов допустимых масштабов и последствий необходима для того, чтобы не допустить перехода от конкуренции в киберпространстве к традиционному военному конфликту.

На дипломатическом треке России необходимо и далее наращивать усилия по продвижению универсальных правил поведения в киберпространстве в рамках переговорного процесса на

[160] Аптекман А. [и др.] Цифровая Россия: новая реальность // Digital McKinsey : сайт. 2017. 133 с. URL:: https://www.mckinsey.com/ru/~/media/McKinsey/Locations/Europe%20and%20Middle%20East/Russia/Our%20Insights/Digital%20Russia/Digital-Russia-report.pdf (дата доступа: 28.02.2021).

уровне ООН.

Ещё в 1998 г. Россия впервые внесла в повестку дня Организации Объединённых Наций вопрос о международной информационной безопасности (МИБ)[161], представив проект резолюции под названием «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» на заседании Первого комитета Генеральной Ассамблеи. Также, именно по инициативе России в 2004 г. была создана Группа правительственных экспертов ООН (ГПЭ ООН) в сфере информатизации и телекоммуникаций в контексте международной безопасности с целью решения проблем международной информационной безопасности. За все время по итогам работы ГПЭ было принято три доклада – Доклады ГПЭ ООН от 2010, 2013 и 2015 гг.[162] В группу входили как Россия, так и США. В 2017 г. работа ГПЭ ООН в сфере информатизации и телекоммуникаций в контексте международной безопасности завершилась полным провалом.

В конце 2018 г. в рамках ООН параллельно было создано сразу два переговорных формата по вопросу решения проблем международной информационной безопасности. Первый – ГПЭ ООН, которая была воссоздана в соответствии с американской инициативой. Второй формат – Рабочая группа открытого состава (РГОС) по достижениям в области информации и телекоммуникаций в контексте международной безопасности – была создана в соответствии с российской инициативой. При этом, и Россия и США принимают участие в работе сразу двух групп.

Однако, по этому треку положительных сдвигов касательно позитивного взаимодействия России и США для решения вопросов международной информационной безопасности ждать не приходится.

Как представляется, факт одновременного создания и функционирования двух альтернативных структур по обеспечению международной информационной безопасности в рамках ООН является лишь отражением той полярности, которую занимают сегодня по отношению к друг другу Россия и США в рассматриваемом вопросе. Так, «американская» ГПЭ является закрытой структурой и включает в себя ограниченный круг государств, в то время как «российская» РГОС исповедует мультистейкхолдеровый подход и предполагает участие абсолютно всех заинтересованных сторон – как государств, так и академических и бизнес кругов.

Подтверждением дальнейшей поляризации может служить прошедшее 9 ноября 2020 г. голосование в Первом комитете 75-й сессии Генеральной Ассамблей ООН по российскому проекту резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», и по американскому проекту резолюции «Поощрение ответственного поведения государств в киберпространстве в контексте международной

[161] Здесь и далее в некоторых моментах будет употребляться термин международная информационная без-опасность (МИБ) в контексте рассуждений о российских международных инициативах, так как именно этот термин активно используется Россией на международной арене и во внутренних обсуждениях рас-сматриваемой проблемы на официальном уровне.

[162] Бойко С. Группа правительственных экспертов ООН по достижениям в сфере информатизации и теле-коммуникаций в контексте международной безопасности: взгляд из прошлого в будущее // Междуна-родная жизнь. 2018. № 8. С. 60-61, 64, 67. URL: https://interaffairs.ru/virtualread/ia_rus/82016/files/assets/downloads/publication.pdf (дата обращения: 17.10.2020); Зинченко А. В., Толстухина А. Ю. Мир или война в киберпространстве?

России не стоит ждать позитивных подвижек в рамках взаимодействия с США, более эффективной политикой будет сохранения продвижения мультстейкхолдерового подхода при обсуждении проблем международной информационной безопасности

безопасности». Данное голосование обнажило политические разногласия вокруг киберповестки, так как принятие российского проекта резолюции вызвало противодействие со стороны Вашингтона по причине продвижения Россией «авторитарной модели для киберпространства»[163].

Представляется, что США при Джо Байдене также «активизируют усилия по установлению всеобъемлющих кибернорм»[164], однако данные инициативы будут подчёркнуто противопоставляться российским инициативам, а российские инициативы, в свою очередь, будут блокироваться.

Поэтому, говоря о необходимости России и далее наращивать усилия по продвижению универсальных правил поведения в киберпространстве в рамках переговорного процесса на уровне ООН, можно иметь в виду прежде всего популяризацию своей модели обеспечения МИБ и втягивания в свою «орбиту» как можно большее количество участников. Пока ГПЭ остаётся закрытым форумом, России вместе с единомышленниками по РГОС стоит и далее продвигать мультстейкхолдеровый подход к обсуждению проблем международной информационной безопасности. Подобная открытость привлечёт внимание более широкого круга субъектов международных отношений к российским инициативам.

Что касается двустороннего формата взаимодействия, то здесь тем более ожидать позитивных подвижек не стоит. Россия и США достигли «пика» во взаимоотношениях по вопросу киберповестки в 2013 г., когда на саммите G8 в Северной Ирландии на двусторонней встрече лидеры стран Владимир Путин и Барак Обама заключили договорённости «О мерах укрепления доверия в сфере использования ИКТ»[165]. Однако, достигнутые в ходе этих переговоров результаты были перечёркнуты политическим кризисом на Украине, а после окончательно «добиты» взломами серверов Национального комитета Демократической партии США во время предвыборной кампании 2016 г. и обвинениями России в их осуществлении.

Например, согласно тому же докладу Госдепартамента США «О международной безопасности в киберпространстве» – сугубо антироссийскому документу, который, скорее всего, тоже будет принят во внимание новой администрацией – вышеописанные «горячие линии» прекратили своё действие из-за «осуществления Россией компании по влиянию, направленной на президентские выборы в США в 2016 г.»[166]. Именно с этого момента произошла утрата всякого доверия между Кремлём и Белым домом – в том числе и по киберповестке. Ну а после вышеописанной киберкампании Sunbirst, в которой также была обвинена Россия, нормализовать взаимодействие с США при Джо Байдене будет крайне тяжело. Любые договорённости, если они были бы достигнуты, могут

[163] Шакиров О. И. Двойная кибербезопасность в ООН // ПИР-Центр : сайт. 2020. URL: http://pircenter.org/blog/view/id/439 (дата обращения: 28.02.2021); Выступление и ответное слово Перво-го заместителя Постоянного представителя Российской Федерации при ООН Д.А. Полянского в Первом комитете 75-й сессии ГА ООН в связи с постановкой на голосование ОР 1 проекта резолюции ГА ООН по МИБ «Достижения в сфере информатизации и телекоммуникаций в контексте международной без-опасности»// Постоянное представительство Российской Федерации при ООН : сайт. 2020. URL: https://russiaun.ru/ru/news/firstcom_0911 (дата обращения: 28.02.2021).

[164] Cyber Policy...

[165] Черненко Е. В. Горячие линии провели в интернет // Коммерсантъ : сайт.2013. URL: https://www.kommersant.ru/doc/2214606 (дата обращения: 17.10.2020).

[166] Ford. C. A. International Security in Cyberspace... P. 6.

снова в любой момент рухнуть из-за очередного политического кризиса между Кремлём и Белым Домом.

Поэтому, здесь возможен вариант перехода к крайне ограниченным и точечным механизмам работы. Речь не идёт о создании каких-либо постоянных рабочих форматах, а лишь о взаимных консультациях «по необходимости» с той целью, чтобы не допустить эскалации киберконфликта и уж тем более его перехода за пределы киберпространства в традиционную область военных действий. Важно таким образом во взаимоприемлемой форме попытаться ограничить военную реакцию на киберинциденты.

Так или иначе, но на данный момент в условиях того, что США видят в России непримиримого соперника – в том числе и в киберсфере, в перспективах применения Соединёнными Штатами стратегии постоянной вовлечённости в отношении России сомневаться не приходится. США «плотно» ввязались в стратегическую конкуренцию по всем фронтам – и киберпространство не исключение.

К сожалению, киберконкуренция – это то, с чем нам придется жить, возможно, ближайшее годы[167].

ЗАКЛЮЧЕНИЕ

Итак, можно видеть, что в последние годы США начинают придерживаться более проактивного и наступательного подхода к обеспечению кибербезопасности. Оформление и актуализация этого подхода, основанного на стратегии постоянной вовлечённости, продолжается до сих пор[168].

Проактивность рассматриваемой стратегии проявляется в том, что США позволяют себе осуществлять упреждающие кибероперации, не достигающие уровня акта агрессии, на постоянной основе и «как можно ближе к источнику предполагаемой атаки», как это видно из рассмотренных выше стратегических документов и примеров.

Также, принятие Соединёнными Штатами стратегии постоянной вовлечённости потребовало не только теоретических, но и политико-институциональных изменений. К таковым изменениям можно отнести повышение статуса Киберкомандования США с подразделения Стратегического командования до полноценного объединенного боевого командования, превращение «Российской малой группы» из временного в постоянно действующее подразделение, отмена директивы Барака Обамы № 20 (PPD-20) и принятие Президентского меморандума о национальной безопасности № 13 (NSPM 13), предполагающего более проактивную политику.

Таким образом, именно при Трампе произошло принятие более конфронтационной стратегии постоянной вовлечённости в киберпространстве, облегчение процедуры одобрения осуществления кибератак в отношении противников Америки и предоставление более широких полномочий Киберкомандованию США[169].

[167] Sokolsky R., Rumer E. U.S.-Russian Relations in 2030. P. 16.
[168] Nakasone P. M., Sulmeyer M. How to Compete in Cyberspace; Kris D. How to Compete in Cyberspace: An Accompaniment [Electronic resource] / Lawfare. Washington, DC, 2020. Mode of access: https://www.lawfareblog.com/how-compete-cyberspace-accompaniment (date of access: 28.10.2020).
[169] Pomerleau M. Is Cyber Command...

Возможно, Джо Байден, предвидя «непредвиденные последствия» от реализации стратегии постоянной вовлечённости, о чём говорилось выше, введёт некоторые ограничения в отношении её применения. Однако в том или ином виде этот курс будет продолжен, о чём свидетельствует само заявление Байдена и тот факт, что он поддержал вышеуказанный Президентский меморандум о национальной безопасности № 13. В совокупности с этим, Вашингтон не собирается взаимодействовать с Россией по вопросу нормализации отношений в сфере кибербезопасности. Возможно, США будут строить систему коллективной безопасности только вместе с союзниками, но против России. Они и дальше будут продвигать собственную модель обеспечения кибербезопасности, которая будет заведомо альтернативна российской. Таким образом, ни в рамках многостороннего, ни в рамках двустороннего формата (тем более), позитивных сдвигов ждать не стоит.

Похоже, что и Россия тоже потеряла надежду нормализовать взаимодействие с США, о чём могут свидетельствовать слова Сергея Рябкова касательно необходимости перехода «к политике сдерживания и избирательного диалога» в отношении Соединённых Штатов[170].

В период стратегической нестабильности и в то время, пока Россия не может договориться с Соединёнными Штатами относительно выработки единых правил поведения в киберпространстве, необходимо учитывать происходящие в стратегии кибербезопасности США изменения, чтобы понимать, как России дальше взаимодействовать с Вашингтоном по вопросу обеспечения международной безопасности. Помимо этого, понимание изменений в концепции кибербезопасности США крайне важно для разработки собственной стратегии противодействия киберугрозам и той политики в сфере обеспечения кибербезопасности, которую Россия будет проецировать на международной арене. ■

[170] Сергей Рябков: Россия в отношениях с США...

ИНДЕКС БЕЗОПАСНОСТИ

Индекс Безопасности – Научные записки – доклады, аналитические статьи, комментарии и интервью, которые отражают позиции российских и зарубежных экспертов по актуальным вызовам глобальной безопасности и политики России в этой сфере. Задача серии – дать понятный анализ проблем международной безопасности и предложить для них конкретные и реалистичные решения. Серия пришла на смену журналу *Индекс Безопасности*, издаваемому ПИР-Центром в 1994 – 2016 гг. Авторы и редакторы серии будут рады комментариям, вопросам и предложениям, которые читатели могут направить на электронную почту inform@pircenter.org

ГЛОБАЛЬНОЕ УПРАВЛЕНИЕ ИНТЕРНЕТОМ И МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Данная научная записка выполнена в рамках проекта «Глобальное управление интернетом и международная информационная безопасность», которая является частью программы ПИР-Центра «Новые технологии и международная безопасность». В рамках проекта изучаются переговорные процессы по выработке норм для информационного пространства, международное сотрудничество в вопросах, связанных с управлением интернетом, а также вызовы безопасности России и международной безопасности, исходящие из информационного пространства.

Индекс Безопасности – Научные записки

№8 (22), 2021

Сергей Себекин

Новая киберэпоха: как США вступают в глобальную конкуренцию в киберпространстве

Главный редактор: В.А. Орлов

Редактор: Н.С. Дегтярёв

Рецензент: В.Б. Козюлин

Дизайн и компьютерная верстка: Е.Г. Чобанян

В оформлении доклада используется фрагмент гравюры Альбрехта Дюрера «Носорог»

Работа над номером завершена
29 апреля 2021 г.

ПИРПРЕСС