Международные процессы, Том 16, № 3, сс. 157–169
DOI 10.17994/IT.2018.16.3.54.9

ХОЛОДНО — О ГОРЯЧЕМ
Дискуссии

ПОЛИТИКА КИБЕРБЕЗОПАСНОСТИ США
ЭВОЛЮЦИЯ ВОСПРИЯТИЯ УГРОЗ

ИЛОНА СТАДНИК
НАТАЛЬЯ ЦВЕТКОВА
Санкт-Петербургский государственный университет, Санкт-Петербург, Россия

Резюме

Данная статья посвящена американской политике в области кибербезопасности с 1990-х годов по настоящее время. Статья опирается на конструктивистскую теорию международных отношений и берёт за основу дискурс-анализ киберугроз, отражённых в официальных документах и стратегиях США. Конструирование и артикуляция угроз рассматривается в данном случае в качестве определяющего фактора для дальнейшего формулирования политики в области кибербезопасности. Изменение дискурса позволяет проанализировать эволюцию американского подхода к кибербезопасности – акценты менялись вместе с администрациями президентов, однако фокусирование на инфраструктурно-сетевой составляющей безопасности оставалось неизменным. Однако по мере развития и распространения технологий киберугрозы получили сначала социальное, а затем и политическое измерение. В середине 2000-х годов добавилось международное измерение политики обеспечения кибербезопасности, так как пришло осознание того, что киберпространство глобально, а для безопасного и экономически выгодного использования Интернета необходимо выстроить международную систему кибербезопасности. Дискурс киберугроз в американских документах также претерпел изменения. Расширилась и была детализирована их типология, возросло многообразие потенциально опасных субъектов, на межгосударственном уровне стали открыто называться возможные противники. Статья состоит из трёх разделов. В первом разделе проанализированы подходы США к кибербезопасности в конце 1990-х – начале 2000-х годов, когда защита внутренних компьютерных систем и односторонний характер политики в киберпространстве доминировали в представлениях политического истеблишмента США. Следующий раздел посвящён периоду администрации Б. Обамы, когда на повестку дня выходит международное взаимодействие, а политика в области кибербезопасности начинает осуществляться на принципах мультистейкхолдеризма – участия всех заинтересованных сторон, включая бизнес, для создания безопасного киберпространства. Последние два раздела рассматривают произошедший после президентских выборов 2016 г. парадигмальный сдвиг в американском видении кибербезопасности в сторону информационной безопасности – подходу, активно отстаиваемому на международном уровне Россией. Скандал с использованием персональных данных американских пользователей Facebook для таргетирования предвыборной рекламы и пропаганды может стать триггером для закрепления информационного фокуса кибербезопасности в обновлённой американской политике в этой сфере.

Ключевые слова:

кибербезопасность; информационная безопасность; ИКТ; США; суверенитет; управление Интернетом; глобальное управление; президентские выборы.

Дата поступления рукописи в редакцию: 23 апреля 2018 г.
Дата принятия к публикации: 8 октября 2018 г.

Для связи с авторами /Corresponding author
Email: ilona.st94@gmail.com

Соединённые Штаты выступают одним из лидеров в построении информационного общества. Стремительное развитие информационно-коммуникационных технологий (ИКТ) и их нарастающее проникновение во все аспекты жизни не только создают новые возможности, но и делают общество зависимым от стабильного и безопасного функционирования технологий. Это, в свою очередь, порождает потребность в обеспечении комплексной кибербезопасности. ИКТ стали чем-то большим, чем просто инструментом для быстрой и лёгкой передачи информации. Технологии играют ключевую роль в системах контроля и мониторинга в различных секторах экономики и национальной безопасности. Финансовый сектор оказался наиболее уязвимым, потому что его функционирование во многом зависит от работы компьютерных программ и сетей.

С этой точки зрения кибербезопасность – защита компьютерных сетей и сопутствующей инфраструктуры – имеет жизненно важное значение для Соединённых Штатов. В 2010 г. бывший директор Агентства по национальной безопасности (АНБ) М. Макконелл заявил, что «США уже находятся в состоянии информационной войны и проигрывают её» [Роговский 2014: 4]. Приведённая цитата иллюстрирует озабоченность политического истеблишмента Соединённых Штатов текущей ситуацией, когда военные и правительственные сети, а также объекты критической инфраструктуры подвергаются атакам, что приводит к значительному ущербу для экономики и безопасности страны.

Правительство США провело масштабную работу по выработке стратегии, целей, а также ресурсной базы в области политики кибербезопасности. Быстрое изменение ситуации в киберпространстве – появление более совершенных технологий, возникновение новых сильных игроков – привело к гонке вооружений и потребовало незамедлительных ответов, а также гибкости в пересмотре концепции кибербезопасности.

Статья опирается на конструктивистскую теорию международных отношений, поскольку её положения концентрируются на анализе образов, восприятий, стереотипных установок субъектов международных отношений, а во главу угла ставится социальное конструирование реальности [Wendt 1999; Wendt 1995; George 1994; Politics as text...2002; Saco 1999]. Это позволяет анализировать восприятие угроз в качестве побудительной причины изменения с течением времени американской политики в области кибербезопасности. За методологическую основу взят дискурс-анализ официальных документов США. Он позволяет проследить изменение восприятия состояния кибербезопасности в американском политическом истеблишменте. Корпус документов включает в себя прежде всего Стратегии национальной безопасности 2002, 2010 и 2017 годов; специальные стратегии по кибербезопасности; обзор киберполитики, подготовленный для администрации Барака Обамы в 2009 году; материалы слушаний комитета по разведке палаты представителей 2014, 2015 и 2017 годов; президентскую директиву об усилении кибербезопасности федеральных сетей и критической инфраструктуры 2018 года. Выбор круга источников определялся конфигурацией институтов, имеющих наибольшее влияние на политику безопасности в США (президент, Конгресс, министерство обороны и национальной безопасности, разведывательное сообщество).

Согласно положениям постструктурализма, которые используются конструктивистами, дискурс представляет собой набор текстов и речевых конструкций, которые определяют социальный и политический контекст того или иного явления, формируют идеологию или образ мышления [Laclau 1995]. Дискурс информационной безопасности отличается от дискурса кибербезопасности тем, что акцентирует внимание на вопросах суверенитета, устойчивости политических режимов и общественного порядка в условиях конкуренции содержательных повесток дня при освещении политических событий и общественных процессов. Он не исключает инфраструктурно-сетевой уровень, а также

защиты информации в логике классической триады – сохранение её конфиденциальности, целостности и доступности. Правительство США до недавнего времени использовало дискурс кибербезопасности в формулировании своей политики, негативно реагируя на попытки других стран закрепить дискурс информационной безопасности в качестве основного на международном уровне. События 2016–2018 годов изменили ситуацию и отношение Соединённых Штатов по этому вопросу, и этот пересмотр концептуальных установок заслуживает внимания.

Статья состоит из трёх разделов. В первом проанализированы подходы США к кибербезопасности в конце 1990-х – начале 2000-х годов, когда защита внутренних компьютерных систем и односторонний характер политики в киберпространстве доминировали в представлениях политического истеблишмента США. Последующие разделы посвящены периодам правления администраций Б. Обамы и Д. Трампа, когда на повестку выходит международное взаимодействие, а политика в области кибербезопасности начинает осуществляться на принципах *мультистейкхолдеризма* – участия всех заинтересованных сторон, включая бизнес, для создания безопасного киберпространства. Последний раздел рассматривает произошедший после президентских выборов 2016 г. парадигмальный сдвиг в американском видении кибербезопасности в сторону информационной безопасности – подходу, активно отстаиваемому на международном уровне Россией.

1

Начиная с 1990-х годов вопросы кибербезопасности появились в повестке дня обеспечения национальной безопасности США. В тот период стратегические документы и исполнительные директивы были ориентированы на обеспечение безопасности внутренних компьютерных сетей, а также безопасности самой информации. При этом последний вызов понимался в рамках классической триады – поддержания целостности, конфиденциальности и доступности данных.

После прихода к власти администрации Дж. Буша-мл. вопросы кибербезопасности стали получать закрепление в основополагающих документах внешней политики Соединённых Штатов. Стратегия национальной безопасности США 2002 г. указывала на возрастающую значимость информационной и кибербезопасности: «прогресс в области науки и технологий настолько сильно изменил ситуацию, что даже небольшая группа людей может угрожать жизни и процветанию большой части населения или всей страны»[1].

Между тем правительство США принялось энергично внедрять опору на компьютерные сети в системы управления. Следовательно, значимость кибербезопасности для правительства возросла: необходимо было избежать попыток проникновения в правительственные сети или нестабильности в их работе, а также несанкционированного доступа к конфиденциальной информации. За последующие годы накопилось столь большое число инцидентов[2], что потребовался пересмотр политики в целях построения эффективной системы управления, способной противостоять нарастающим вызовам и обеспечивать сохранение американского господства в сфере использования ИКТ.

В начале 2000-х годов Интернет стал часто фигурировать в документах, содержащих отсылки к киберугрозам США. В национальной стратегии по безопасному киберпространству было признано, что американская «экономика и национальная

[1] National Security Strategy, Bush Administration, 2002. URL: http://georgewbush-whitehouse.archives.gov/nsc/nss/2002/

[2] Significant Cyber Incidents since 2006, Center for Strategic and International Studies. URL: https://csis-prod.s3.amazonaws.com/s3fs-public/180425_Significant_Cyber_Events_List.pdf?pqetcWcwV7mvAo33_lAZFlQVQz7.EOqh

безопасность полностью зависят от информационных технологий и информационной инфраструктуры; основу этой информационной инфраструктуры составляет Интернет»[3]. В этой связи документ был нацелен на укрепление кибербезопасности инфраструктуры, поддерживающей банки и финансовые операции; правоохранительные органы; образование; социальное страхование; управление электроэнергией, водоснабжением, транспортом. Именно в это время появляется идея государственно-частного партнёрства в области обеспечения кибербезопасности, которая получила широкое признание впоследствии.

Кроме того, упомянутая стратегия интересна тем, что в ней впервые было дано определение киберугрозам. К ним были отнесены атаки на критическую информационную инфраструктуру[4]. Были выделены следующие типы угроз: внутренние угрозы, исходящие от сотрудников, которые имеют доступ к информационным системам и компьютерным сетям, а значит, могут использовать свой статус в преступных целях; хакерские атаки, совершённые ради удовольствия или со злым умыслом; хактивизм – политически мотивированные атаки на веб-сайты, серверы, информационные системы; *распространение вредоносного программного обеспечения или кода; кража личных данных и финансовые преступления; DDoS-атаки; кибершпионаж*, проводимый зарубежными спецслужбами[5].

2

В период правления Б. Обамы вопросам защиты правительственных организаций от кибератак стало уделяться ещё больше внимания, а в Стратегии национальной безопасности 2010 г. появился отдельный параграф, специально посвящённый этому вопросу. В нём указывалось, что «технологии способствуют нашему военному превосходству, но наши несекретные правительственные сети постоянно подвергаются взломам. Наша повседневная жизнь и общественная безопасность зависят от работы энергосистем, но потенциальные противники могут использовать киберуязвимость, чтобы нарушить их функционирование в огромном масштабе. Интернет и электронная коммерция являются ключом к конкурентоспособности нашей экономики, но из-за киберпреступлений компании и потребители теряют сотни миллионов долларов, а также ценную интеллектуальную собственность»[6]. В документе говорится, что США должны укреплять механизмы международного сотрудничества в области кибербезопасности, включая разработку международных стандартов и норм ответственного поведения государств, совершенствование законодательства по борьбе с киберпреступностью и пиратством, защите данных, расследованию и реагированию на киберинциденты и нападения[7]. Подход администрации Обамы по укреплению кибербезопасности включал в себя следующие принципы: приоритет защиты сетей, защиту частной жизни и гражданских свобод, государственно-частное сотрудничество по обеспечению кибербезопасности[8].

Международное сотрудничество было нацелено на создание «функционально совместимого, безопасного и надёжного киберпространства» с участием всех заин-

[3] National Strategy to Secure Cyberspace, the White House, February 2003. Available at: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

[4] Ibid.

[5] Statement for the record of Louis Freeh, Director FBI on cybercrime before the Senate Committee on Appropriations Subcommittee for the Department of Commerce, Justice, State and Judiciary. Washington D.C., February 16, 2000.

[6] National Security Strategy. Obama administration, 2010. URL: https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[7] The Obama's Administration's Priorities on Cybersecurity, The White House. URL: https://obamawhitehouse.archives.gov/node/233081

[8] The Obama's Administration's Priorities on Cybersecurity, The White House. URL: https://obamawhitehouse.archives.gov/node/233081

тересованных сторон – *мультистейкхолдеризм* – в управлении Интернетом и без ограничений свободного доступа к нему.

Именно администрация Б. Обамы стала развивать политику международного взаимодействия в данной области. Международная стратегия по киберпространству, опубликованная в 2011 году, определила дополнительные угрозы кибербезопасности. *Во-первых*, в ней подчёркивалась важность «свободного потока информации, безопасность и конфиденциальность данных и целостность взаимосвязанных сетей» для американского и глобального экономического процветания, и безопасности[9]. *Во-вторых*, она заостряла внимание на физических угрозах для сетей и сопутствующей инфраструктуры (кабели, серверы, беспроводные средства), включая стихийные бедствия или техногенные катастрофы. Назывались и конкретные угрозы: вымогательство, мошенничество, кража персональных данных и интеллектуальной собственности. Такие действия могут подрывать доверие пользователей к электронной торговле, социальным сетям и даже их личной безопасности[10]. Ещё одной причиной для беспокойства было названо блокирование веб-сайтов в некоторых странах.

Указанные стратегические документы США отражают смещение акцента с внутренней безопасности компьютерных сетей на экономически и социально ориентированную политику в области кибербезопасности с международными амбициями в 2000-х годах.

Реализация подходов администрации Б. Обамы в области международного взаимодействия по обеспечению кибербезопасности столкнулась с рядом трудностей. Директор национальной разведки США Дж. Клэппер на слушаниях в Палате представителей назвал основные причины, препятствовавшие осуществлению американских планов. Расхождения Соединённых Штатов с Россией и Китаем по вопросам кибербезопасности рассматривались в качестве основной проблемы. По мнению американского чиновника, эти две страны выступали противниками США в области кибербезопасности, отстаивая собственное понимание суверенитета в киберпространстве, подразумевавшее контроль над Интернетом и введение цензуры. В качестве ещё одной угрозы США рассматривали наращивание наступательных кибервооружений в России, Китае, Иране и Северной Корее[11].

Тем не менее США не ожидали каких-то серьёзных атак в стиле «кибер Пёрл-Харбор», а предполагали возможность серий инцидентов «низкого и среднего уровня, исходящих из различных источников[12]. Такого рода опасения нашли отражение и в стратегии кибербезопасности Пентагона. Американские военные также подчёркивали, что основными объектами нападения могут стать частные лица или компании, а также промышленные системы[13]. В то же время стратегия Министерства обороны США не исключала возможность использования кибератак в качестве политического инструмента[14].

Между тем ЦРУ разработало свою классификацию источников (субъектов), которые могут угрожать безопасности США: государства с развитыми программами в области кибервооружений и разведки (такие как Россия или Китай); государства с меньшими техническими возможностями, но, предположительно, с более агрессивными намерениями (например, Иран и

[9] The U.S. International Strategy for Cyberspace, The White House, May 2011, Washington D.C.
[10] The U.S. International Strategy for Cyberspace, The White House, May 2011, Washington D.C.
[11] Worldwide threat assessment. James R. Clapper, testimony to House Permanent Select Committee on Intelligence, February, 2014.
[12] Worldwide threat assessment. James R. Clapper, testimony to House Permanent Select Committee on Intelligence, February, 2014.
[13] What's new in the U.S. cyber strategy. The Washington Post, April 24, 2015.
[14] The DoD Cyber Strategy. April 2015. URL: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Северная Корея); преступники, ориентированные на получение прибыли; идеологически мотивированные хакеры или экстремисты.

Таким образом, Россия и Китай были обозначены основными источниками угроз в период правления Б. Обамы. В частности, США выражали беспокойство инициативами Москвы по реформированию международной системы управления Интернетом, что подразумевало наделение правительств большими полномочиями и передачу функций регулирования киберпространства межправительственной организации. Такая реформа представлялась не совместимой с американскими ценностями и интересами[15]. Кроме того, по оценкам американских ведомств, российские спецслужбы получали доступ к конфиденциальной информации в компьютерных сетях Соединённых Штатов.

В случае с Китаем обеспокоенность США вызывали попытки регулирования поведения пользователей Интернета, собственная интерпретация модели управления Всемирной сетью, а также инциденты взлома американских сетей с целью кражи интеллектуальной собственности или конфиденциальной информации[16]. Так же как и в случае с Россией, американо-китайские расхождения по вопросам кибербезопасности осложнялись разницей в нормативных представлениях – в том числе разными взглядами на свободу Интернета, его регулирование, а также феномен киберпреступности [Wenli 2013].

На фоне усиления опасений относительно межгосударственного противоборства среди неправительственных объединений только ИГИЛ (организация, запрещённая в России) была признана террористической организацией, использующей киберпространство для «вербовки боевиков и распространения пропаганды»[17]. Кроме того, использование атак на информационные системы и ресурсы идеологически мотивированными группами для достижения политических целей продолжало восприниматься в качестве серьёзной угрозы.

Наконец, правительство США стало выделять новый тип проблем в киберпространстве – гибридные угрозы, исходящие от государственных и негосударственных игроков: «группировки, вдохновлённые патриотическими чувствами, часто подменяют собой государства при совершении атак; негосударственные игроки могут обеспечить прикрытие для государственных операций»[18]. Такое поведение усложняет проблему атрибуции кибератак – выявления их источника.

3

С приходом к власти Д. Трампа тема кибербезопасности в политическом истеблишменте не потеряла актуальности. Интерес подогревался не только утечками архивов документов, содержащих данные об американских кибервооружениях, но и инициативами, выдвинутыми новым президентом и его командой [Демидов 2017]. В первую очередь в СМИ попал проект Директивы об усилении кибербезопасности США[19]. Документ прояснял акценты новой администрации применительно к тематике кибербезопасности. Из него следует, что президент Д. Трамп размышлял над пересмотром национальной политики в этой области. Документ закреплял

[15] Worldwide threat assessment. James R. Clapper, testimony to House Permanent Select Committee on Intelligence, February, 2014.

[16] Worldwide threat assessment. James R. Clapper, testimony to House Permanent Select Committee on Intelligence, February, 2014.

[17] The DoD Cyber Strategy. April 2015. URL: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[18] The DoD Cyber Strategy. April 2015. URL: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[19] Executive order – Strengthening U.S. Cyber Security and Capabilities (Draft). The Washington Post. Available at: https://apps.washingtonpost.com/g/documents/world/read-the-trump-administrations-draft-of-the-executive-order-on-cybersecurity/2306/

Интернет в качестве «жизненно необходимого национального ресурса», в связи с чем США планировали «формировать киберпространство наряду с другими международными, государственными и негосударственными игроками», но оставляли за собой право использовать весь спектр своих возможностей, чтобы защитить американские интересы. Такая формулировка ясно свидетельствовала о желании Соединённых Штатов сохранять и укреплять доминирующее положение в том, что касается использования и регулирования киберпространства. Администрация Д. Трампа оперировала такими понятиями, как *киберуязвимость*, *киберпротивники* и *кибервозможности*. Под последним понимался сбор информации об американских специалистах, которые могут содействовать политике США по защите компьютерных систем и данных.

Однако утверждённая 11 мая 2018 г. финальная версия директивы сместила фокус на укрепление кибербезопасности сетей агентств и подразделений федеральной исполнительной власти США[20]. Большое внимание уделялось риск-менеджменту и прямой ответственности глав основных федеральных агентств за управление киберрисками ведомственных сетей. Кроме того, исполнительная власть обязывалась поддерживать владельцев и операторов национальной критической инфраструктуры в управлении рисками в отношении их объектов. Директива также предусматривала предоставление отчётов в течение одного-полутора месяцев с момента её утверждения о состоянии кибербезопасности различных отраслей, о вариантах сдерживания противников и защиты американского народа от киберугроз и об инициативах сотрудничества с зарубежными ведомствами с целью расследования киберинцидентов, обмена информацией и содействия в атрибутировании атак.

Такая практика схожа с подходами времён администрации Б. Обамы, в ходе правления которой Министерство внутренней безопасности США составило обзор политики кибербезопасности, предложило назначить лицо, ответственное за межведомственную координацию в этой области, а также ряд других кадровых и организационных новшеств[21]. Администрация Д. Трампа начала менять сложившуюся структуру. Изменения начались с Государственного департамента, в котором был упразднён пост координатора по киберпространству. Этот шаг подвергся критике как ослабляющий позиции США в кибердипломатии. В этой связи в Конгресс на рассмотрение был внесён законопроект, который предполагал создание в Госдепартаменте отдельного бюро, ответственного за работу в киберпространстве, и обязывал государственного секретаря выпустить новую международную стратегию, определяющую проведение американской внешней политики в Интернете[22]. Аналитики считают, что такого рода акт может иметь законодательную перспективу [Cameron 2017]. Наконец, Советник по национальной безопасности США анонсировал подготовку новой национальной стратегии кибербезопасности взамен документов предыдущей администрации[23].

Стратегия национальной безопасности, опубликованная в декабре 2017 года, также

[20] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. The Wight House, May 11, 2018. URL: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[21] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. Department of Homeland Security, 2009. URL: https://www.dhs.gov/publication/2009-cyberspace-policy-review

[22] H.R.3776 – Cyber Diplomacy Act of 2017, 115th Congress (2017-2018) URL: https://www.congress.gov/bill/115th-congress/house-bill/3776/text

[23] Trump Administration Plans a New Cybersecurity Strategy. Nextgov, October 24, 2017. URL: https://www.nextgov.com/cybersecurity/2017/10/trump-administration-plans-new-cybersecurity-strategy/142014/

содержала ряд важных упоминаний о намерениях администрации Д. Трампа по обеспечению кибербезопасности США. *Во-первых*, в соответствии с документом защита национальной критической инфраструктуры и правительственных сетей должна осуществляться по проактивному принципу: возникающие угрозы необходимо предвидеть и предотвращать, а не устранять последствия кибератак. Для этого США будут инвестировать в улучшение методик атрибутирования кибератак, а также вводить серьёзные санкции в отношении иностранных правительств, преступников и других игроков, осуществляющих вредоносную деятельность. *Во-вторых*, в стратегии обозначены основные типы угроз Соединённым Штатам. Указывается, что: «государственные и негосударственные игроки используют кибератаки для вымогательства, ведения информационных войн и распространения дезинформации. <...> Такие атаки способны нанести ущерб большому числу людей и учреждений <...> и подорвать веру и доверие к демократическим институтам и глобальной экономической системе. Многие страны в настоящее время рассматривают киберпотенциал как инструмент для распространения своего влияния, а некоторые используют возможности киберпространства для консолидации своих автократических режимов»[24].

Примечательно, что Стратегия национальной безопасности 2017 г. стала первым концептуальным документом США, в котором упоминается информационная война как угроза нормальному функционированию демократических институтов в связке с кибербезопасностью. Это свидетельствовало о появлении нового дискурса – в тексте вопросы безопасности информационного пространства трактовались в контексте защиты национального суверенитета. Помимо этого, документ позиционировал США как защитника киберпространства от вредоносных действий, а также защитника Интернета в том виде, каким он задумывался изначально – на принципах доверия и открытости, свободы от цензуры и блокировок.

В отличие от предыдущих администраций, Д. Трамп и его команда обозначали частный сектор как источник эффективных решений для защиты киберпространства. Соответственно, задача правительства виделась в том, чтобы сделать выгодным для компаний обеспечение кибербезопасности. Экспертное сообщество в этой связи к основным киберугрозам отнесло утечки конфиденциальной информации вследствие кибершпионажа, риски сохранности персональных данных, политически мотивированные кибератаки и атаки на критическую инфраструктуру с разрушительным потенциалом [Cyber recommendations... 2017].

Участившиеся случаи громких кибератак на крупные корпорации, правительственные сети и гражданские объекты критической инфраструктуры[25] свидетельствуют о том, что до сих пор США и другие государства не решили задачу создания успешной системы наказания иностранных игроков за киберпреступления на их территории. Соединённые Штаты с самого начала обсуждения на межправительственном уровне (например, в рамках группы правительственных экспертов ООН по вопросам использования ИКТ в контексте международной безопасности) проводили политику, направленную на имплементацию принципов ответственного поведения государств. Многолетние переговоры по этому вопросу затягиваются в силу отсутствия согласия России и Китая – двух стран со сравнимым киберпотенциалом. Возрастающая роль частного сектора в киберпространстве также влияет на амери-

[24] National Security Strategy. The White House, December 2017. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

[25] Например, см.: Sony Pictures: Inside the Hack of the Century. Fortune, June 25, 2015. Massive Data Breach Puts 4 Million Federal Employees' Records At Risk. NPR, June 4, 2015 Кибератака стала причиной обесточивания Украины. МИР 24. 10 января, 2016.

канскую политику. Корпорации сами выдвигают международные инициативы по созданию приемлемых для них норм обеспечения кибербезопасности[26].

Для администрации Трампа стало очевидным, что фокусирование исключительно на вызовах кибербезопасности с территории самих Соединённых Штатов, как это было в первой половине 2000-х годов, будет равносильно борьбе с ветряными мельницами. Она стремится к изменению поведения как государственных, так и частных (корпоративных) игроков в киберпространстве. В этом контексте представляются уместными классические стратегии сдерживания, а также более мягкие меры, включающие в себя инновации, экономическое влияние, ответные санкции, преследование нарушителей в судах [Nye 2017].

4

Привлечению широкого общественного внимания к вопросам безопасности в Интернете способствовала кибератака на Национальный демократический комитет в июне 2016 года, приведшая к утечке корреспонденции кандидата на пост президента Х. Клинтон и сотрудников её предвыборного штаба. Материалы украденного массива были опубликованы на сайте *WikiLeaks* в преддверии съезда Демократической партии США. Ранее высказывавшиеся опасения стали реальностью – кибератаки превратились в нешуточный политический инструмент. В одночасье Соединённые Штаты столкнулись с новой формой киберугрозы – атака на организации, связанные с проведением выборов. По словам конгрессмена от Демократической партии Адама Шиффа, США подверглись «беспрецедентному вторжению и попытке повлиять или даже нарушить их основополагающий политический процесс»[27].

Незамедлительно последовала серия расследований, выводы которых были озвучены сначала на экспертном уровне (что привело к увязыванию источника атаки с Россией)[28], а затем и в выступлениях руководства ответственных ведомств. В совместном заявлении Директора Национальной разведки и Агентства внутренней безопасности США утверждалось, что «российское правительство причастно к краже переписки и её публикации в целях вмешательства в американский избирательный процесс»[29]. При этом представители американских спецслужб подчёркивали, что путём вторжения в сети невозможно повлиять на конечный результат выборов, независимо от того, стоит ли за ним иностранное правительство или хакерские группировки. Этот же тезис был повторён Национальной ассоциацией государственных секретарей штатов (*National Assocation of Secretaries of State*), в сферу деятельности которых входят вопросы организации избирательного процесса. В их официальном заявлении сказано, что выборные системы в ноябре 2016 г. не были затронуты кибератаками[30]. Несмотря на то что летом того же года были выявлены и подтверждены ФБР две попытки получения доступа к базам регистрации избирателей в Аризоне и Иллинойсе, системы подсчёта голосов не

[26] The need for a Digital Geneva Convention. Microsoft, February 14, 2017. URL: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#KDKc2EJAhl0ykwvk.99

[27] U.S. investigating potential covert Russian plan to disrupt November elections. The Washington Post, September 6, 2016.

[28] Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector Release. Department of Homeland Security, January 6, 2017. URL: https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

[29] Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security, October 07, 2016. URL: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

[30] Key Facts and Findings on Cybersecurity and Foreign Targeting of the 2016 U.S. Elections. National Association of Secretaries of States, March 20, 2017. URL: http://www.nass.org/index.php/index.php/component/docman/?task=doc_download&gid=1923&Itemid=829

пострадали. Более того, Ассоциация подчёркивала, что инфраструктура обеспечения избирательного процесса в США децентрализована, то есть не имеет единой системы, хакерский взлом которой мог бы привести к подрыву выборов.

Впрочем, эти заключения не помешали министру внутренней безопасности США Джею Джонсону внести американские избирательные системы в перечень национальной критической инфраструктуры, поскольку они «играют ключевую роль в жизни нашей страны»[31]. Обеспечение объектов этого типа регулируется федеральными законами. В конце марта 2017 г. в комитете по разведке Палаты представителей прошли слушания, в которых принимали участие Директор Агентства национальной безопасности (АНБ) Майкл Роджерс и директор ФБР Джеймс Комей. Общим лейтмотивом их выступлений стало утверждение, что атака, приведшая к публикации конфиденциальной переписки Х. Клинтон в ходе предвыборной кампании, нарушила американский суверенитет. Она повлияла на «самый священный акт демократии» – выборы[32].

Однако инциденты со взломами почтовых серверов и баз избирателей стали лишь верхушкой айсберга. В феврале 2018 г. стало известно о деятельности компании *Cambridge Analytica*, которая получила доступ к персональным данным от 50 до 87 млн американских граждан (по разным оценкам) через приложение для прохождения персональных тестов в социальной сети *Facebook*[33]. Эти сведения, согласно возникшим в Соединённых Штатах предположениям, могли быть переданы российскому Агентству интернет-исследований, которое использовало их для таргетирования рекламы в пользу Д. Трампа во время предвыборной кампании. Тем самым российская организация подозревалась во вмешательстве в американские выборы путём дискредитации кандидатуры Х. Клинтон[34]. Позднее ей были предъявлены соответствующие обвинения[35].

Общественный резонанс заставил главу *Facebook* Марка Цукерберга публично признать утечку персональных данных пользователей. После этого глава компании был приглашён для дачи показаний на слушаниях в Сенате, а затем и в Палате представителей США. Перед ним были поставлены вопросы конфиденциальности персональных сведений. Кроме того, американские законодатели потребовали прояснить ситуацию с распространением российской пропаганды в социальной сети во время выборов. Анализ формулировок политиков во время слушаний позволяет говорить об изменениях в дискурсе кибербезопасности США в сторону признания проблемы влияния информационного контента на безопасность страны[36].

* * *

Представление о кибербезопасности в США прошли несколько ступеней эволюции. Если в конце 1990-х – начале 2000-х годов внимание уделялось в основном вопросам обеспечения внутренней безопас-

[31] Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector Release. Department of Homeland Security, January 6, 2017. URL: https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

[32] The real winner of the House Intelligence Committee hearing on Russia. The Washington Post, March 23, 2017.

[33] Facebook scandal 'hit 87 million users'. BBC, 4 April 2018. URL: http://www.bbc.com/news/technology-43649018

[34] Цукерберг не нашёл связи между Россией и помогавшими Трампу аналитиками. РБК, 22 марта, 2018; Mark Zuckerberg Talks to WIRED About Facebook's Privacy. WIRED, March 21, 2018.

[35] Internet Research Agency Indictment. The U.S. Department of Justice, February 16, 2018. Available at: https://www.justice.gov/file/1035477/download

[36] Transcript of Mark Zuckerberg's Senate hearing. The Washington Post, April 10, 2018. URL: https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.27af83b8b011

ности сетей с акцентом на технических вопросах, то по мере развития и распространения технологий киберугрозы получили сначала социальное, а затем и политическое измерение.

Вторая половина 2000-х годов ознаменовалась усилением международного компонента политики обеспечения кибербезопасности, так как пришло осознание того, что киберпространство глобально, а для безопасного и экономически выгодного использования Интернета необходимо выстроить международную систему. В официальных документах начали встречаться упоминания о внешних игроках как об оппонентах США в вопросах формирования глобальной системы кибербезопасности – в первую очередь о России и Китае.

Дискурс киберугроз в американских документах также претерпел изменения. Расширилась и была детализирована их типология, возросло многообразие потенциально опасных субъектов, на межгосударственном уровне стали открыто называться возможные противники. Наконец, хакерская атака на Национальный демократический комитет накануне президентских выборов в США, а также скандал с утечкой данных в *Facebook* привели к принципиальному изменению дискурса киберугроз: в американском политическом истеблишменте впервые заговорили о нарушении суверенитета страны в результате воздействия зарубежной пропаганды.

Долгие годы основной причиной разногласий с Россией и Китаем служил вопрос обеспечения суверенитета в киберпространстве. Именно российская концепция информационной безопасности опиралась на обоснование угрозы применения ИКТ для подавления политической независимости государства. Во второй половине 2010-х годов американский истеблишмент начал оперировать схожими категориями, заявляя, что произошло вмешательство во внутриполитические процессы, повлиявшее на исход президентских выборов.

Станет ли это триггером для изменения американской стратегии кибербезопасности во время президентства Д. Трампа? Признают ли США жизнеспособность концепции информационного суверенитета и изменят свои внешнеполитические принципы в отношении кибербезопасности? От возможных ответов на эти вопросы будет зависеть дальнейшее развитие взаимодействия с Россией и Китаем в области международной кибербезопасности.

Список литературы

Демидов О. ЦРУ везде и всюду. Что мы узнали о кибермире из очередной утечки Wikileaks // Россия в глобальной политике, 21 марта 2017. URL: http://www.globalaffairs.ru/global-processes/TcRU-vezde-i-vsyudu-18633

Роговский Е.А. Кибер-Вашингтон: глобальные амбиции. М.: Международные отношения, 2014. 848 с.

Cameron K. Cyber Diplomacy Act gives cyber the importance it needs at the State Departmentю Brookings Institution, December 4, 2017 URL: https://www.brookings.edu/blog/techtank/2017/12/04/cyber-diplomacy-act-gives-cyber-the-importance-it-needs-at-the-state-department/

Cyber recommendations for Next Administration: From Awareness to Action. CSIS, January, 2017. URL: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf

George J. Discourses of Global Politics: A Critical (Re) Introduction to International Relations. Boulder: Lynne Rienner. 1994. 226 P.

Laclau E. Discourse, [in:] R.E. Goodin, P. Pettit (eds.), A Companion to Contemporary Political Philosophy, Blackwell Publishers Ltd, Oxford, 1995. P. 541–547.

Nye J. Deterrence and Dissuasion in Cyberspace // International Security. Vol. 41. No. 3 (Winter 2016/17). P. 44–71.

Politics as Text and Talk. Approaches to Political Discourse. Ed.: P. Chilton, C. Schäffner. Amsterdam: John Benjamins, 2002. 256 p.

Saco D. Colonizing Cyberspace: "National Security" and the Internet // Cultures of Insecurity: States, Communities, and Danger / ed. by J. Weldes, M. Laffey, R. Duvall, H. Gusterson. Minneapolis: University of Minnesota Press, 1999. P. 268–272.

Wendt A. Constructing International Politics // International Security. 1995. Vol. 20. No. 1. P. 71–81.

Wendt A. Social Theory of International Politics. Cambridge: Cambridge University Press, 1999. 447 p.
Yi Wenli. Divergence and Co-operation between China and the U.S. on the Cyberspace Issue // Contemporary International Relations. Vol. 22. No. 4. 2012. P. 124–141.

UNITED STATES CYBERSECURITY POLICY
THE EVOLUTION OF THREAT PERCEPTIONS

ILONA STADNIK
NATALIA TSVETKOVA
Saint Petersburg State University, Saint Petersburg 191060, Russia

Abstract

This article examines the American policy in the field of cybersecurity since the 1990s to the present. The article is based on the constructivist theory of international relations and takes as a basis the discourse analysis of cyber threats reflected in U.S. official documents and strategies. The construction and articulation of cyber threats are, in this case, the founding factors for the further formulation of cybersecurity policy. Changes in the discourse of cyber threats allow us to analyze the evolution of the American approach to cybersecurity, notably the weights in the documents followed the changes of the presidential administrations, but the main focus on the infrastructure and network security remained stable. However, with the development and dissemination of technologies cyberthreats had received social and then political dimension. In the mid-2000s appeared the international dimension of cybersecurity policy; it became clear that cyberspace is global, and for the safe and cost-effective use of the Internet it is necessary to build an international cybersecurity system. The discourse of cyber threats in American documents has undergone some changes. Their typology was expanded and detailed, the variety of potentially dangerous actors has increased, and possible rivals have become openly called at the interstate level. The article consists of three sections. The first analyzes the U.S. approaches to cybersecurity in the late 1990s-early 2000s, when the protection of internal computer systems and the unilateral nature of the policy in cyberspace dominated the views of the American political establishment. The next section is devoted to the period of the B. Obama administration, when international cooperation was put on the agenda, and cybersecurity policy started being implemented on the principles of multistakeholderism – the participation of all stakeholders, including business, to create a secure cyberspace. The last two sections consider the paradigm shift in the American vision of cybersecurity towards information security, an approach actively advocated at the international level by Russia, that took place after the 2016 U.S. presidential elections. The scandal with the use of personal data of American users of Facebook for targeting election advertising and propaganda can become a trigger for consolidating the information focus of cybersecurity in the updated American policy.

Keywords:

cybersecurity; information security; ICT; United States; sovereignty; Internet governance; global governance; presidential elections.

References

Cameron K. (2017) *Cyber Diplomacy Act gives cyber the importance it needs at the State Department*. Brookings Institution. URL: https://www.brookings.edu/blog/techtank/2017/12/04/cyber-diplomacy-act-gives-cyber-the-importance-it-needs-at-the-state-department/

Chilton P., Schäffner C. (2002). *Politics as Text and Talk. Approaches to Political Discourse*. Amsterdam: John Benjamins. 256 p.

Cyber recommendations for Next Administration: From Awareness to Action. CSIS, January, 2017. URL: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf

Demidov O. (2017) TSRU vezde i vsyudu CHto my uznali o kibermire iz ocherednoj utechki Wikileaks [CIA is everywhere. What do we know from about the cyber world from the Wikileaks] *Russia in Global Affairs*. URL: http://www.globalaffairs.ru/global-processes/TcRU-vezde-i-vsyudu-18633

George J. (1994) *Discourses of Global Politics: A Critical (Re) Introduction to International Relations.* Boulder: Lynne Rienner. 226 p.

Laclau E. (1995) Discourse. In: R.E. Goodin, P. Pettit (eds.). *A Companion to Contemporary Political Philosophy.* Blackwell Publishers Ltd, Oxford. P. 541–547.

Nye J. (2017) Deterrence and Dissuasion in Cyberspace. *International Security.* Vol. 41. No. 3. P. 44–71.

Rogovskij E. (2014) *Kiber-Vashington: globalnye ambicii.* [Cyber-Washington: global ambitions] Mezhdunarodnye otnosheniya, Moscow. 848 P.

Saco D. (1999) Colonizing Cyberspace: "National Security" and the Internet. In J. Weldes, M. Laffey, R. Duvall, H. Gusterson (eds) *Cultures of Insecurity: States, Communities, and Danger.* Minneapolis: University of Minnesota Press. P. 268–272.

Wendt A. (1995) Constructing International Politics. *International Security.* Vol. 20. No. 1. P. 71–81.

Wendt A. (1999). *Social Theory of International Politics.* Cambridge: Cambridge University Press. 447 p.

Yi Wenli. (2012) Divergence and Co-operation between China and the U.S. on the Cyberspace Issue. *Contemporary International Relations.* Vol. 22. No. 4. P. 124–141.