МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра международных отношений и внешней политики России

Политика США в киберпространстве: государственная стратегия и институты реализации

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

Студентки 4 курса 441 группы

Направления 41.03.05 «Международные отношения»

Института истории и международных отношений

Лукьяненко Весты Владимировны

Научный руководитель

Доц., к.и.н. _____ О.К. Рыбалко
должность, уч. степень, уч. звание подпись, дата инициалы, фамилия

Зав. кафедрой

Проф., д.и.н., проф. _____ Ю.Г. Голуб
должность, уч. степень, уч. звание подпись, дата инициалы, фамилия

Саратов 2020

ВВЕДЕНИЕ

XXI век – это время небывалого инновационного прогресса, век новой технологической революции. Данный факт сказался и на устройстве системы международных отношений. Сейчас ни одно государство мира не может представить свое существование без сети интернет. Экономическое развитие, политическая составляющая, социальная и культурная сферы общества и государств – все это сейчас напрямую зависит от того, насколько хорошо и бесперебойно функционируют информационное и кибернетическое пространства тех самых государств.

Информационно–коммуникационные технологии дают странам большие преимущества, но они также являются и источником большого количества угроз для нормального функционирования государств. Одним из первых государств, осознавших новые информационные реалии мироустройства стали Соединенные Штаты Америки. До сих пор США являются одними из лидеров среди самых технологически развитых государств мира.

Информационно – коммуникационные технологии (ИКТ) в США перестали быть просто системой передачи и приема данных. Теперь это «нервная система» государства, от нее зависят все сферы жизнедеятельности США, при сбое которой американское общество вряд ли сможет нормально функционировать. Американское руководство вовремя распознало эту тенденцию и приступило к разработке схем по обеспечению безопасности в кибернетическом пространстве, которое в новых реалиях превратилось в дополнительное пространство политического сотрудничества и соперничества. В связи с этим, в администрациях президентов США, начиная еще с Б. Клинтона, ведется разработка стратегий и доктрин, призванных стать программным руководством для осуществления политики США в киберпространстве, чтобы эффективно осуществлять свои цели и отстаивать собственные интересы, но одновременно и обеспечивать кибербезопасность общества.

Программные, доктринальные установки США успешно реализуются на практике. Так, США первыми в мире создали специальный государственный орган, отвечающий, как за наступательную, так и за оборонительную политику Соединенных Штатов в киберпространстве – Киберкомандование США.

Актуальность данного исследования обусловлена тем, что в нем анализируются события, которые происходят в данный момент времени. Сейчас жизнедеятельность практически всех государств мира неразрывно связана с киберпространством. Каждый год мы наблюдаем, как происходит развитие межгосударственных отношений в киберпространстве - начиная с киберскандалов и случаев электронного вмешательства в выборы, заканчивая разработкой международной стратегии по ведению кибервойны. В складывающихся условиях необходимо понимать истинную природу происходящего, повышая киберграмотность. Анализ последствий нельзя произвести без понимания истоков и причин происходящего.

В данной работе произведена попытка взглянуть на киберпространство глазами американского руководства, выявить официальные цели американской киберполитики и «дорожную карту» выполнения поставленных целей. Представленные в исследовании данные помогут оценить происходящие в настоящем киберсобытия, основываясь на мнениях разных сторон, принимая во внимание разные точки зрения. Эти знания также способствуют процессу эффективного прогнозирования будущей киберполитики США, что, в свою очередь, может помочь при разработке национальных кибермер.

Степень разработанности темы в научной литературе. В настоящее время существует достаточное количество как отечественных, так и зарубежных экспертных исследований и материалов по теме данной работы.

***Исследования российских авторов*.** Вопросу развития киберполитки США российские эксперты уделяют достаточно много внимания. Стоит отметить, что в отечественных исследованиях прорабатываются не столько

вопросы возможного сотрудничества США и России в киберсфере, сколько подробно изучается внутренняя программа, принимаемая руководством США относительно американской киберполитики. В процессе проведения данного исследования особое внимание уделялось работам таких российских авторов, как И. Стадник и Н. Цветкова[1], Н.В. Кардава[2], Е.В. Журбей[3], А. Медин и С. Маринин[4], Ю. Горбачев[5], А. Ализар[6], В.А. Васенин[7], А.Б. Николаева и М.В. Тумбинская[8].

Зарубежные исследования. Хотелось бы отметить, что в научных работах зарубежных исследователей наибольшее количество внимания уделяется вопросам обеспечения кибербезопасности США, защиты критической инфраструктуры, правительственных компьютерных сетей. Так,

---

[1] Стадник И., Цветкова Н. Политика кибербезопасности США. Эволюция восприятии угроз // Международные процессы, Т.16 № 3. С.157 - 159. URL:http://intertrends.ru/system/Doc/ArticlePdf/2036/XDCkL0o5Ke.pdf (Дата обращения:15.04.2020).

[2] Кардава Н.В. Киберпространство как новая политическая реальность: вызовы и ответы // История и современность. 2018. №1-2. С. 152-166. URL: https://cyberleninka.ru/article/n/kiberprostranstvo-kak-novaya-politicheskaya-realnost-vyzovy-i-otvety (Дата обращения: 09.04.2020).

[3] Журбей Е.В. Стратегия национальной безопасности США в 90-е гг. XX в. // Мировая система и межрегиональные отношения.URL: https://cyberleninka.ru/article/n/strategiya-natsionalnoy-bezopasnosti-ssha-v-90-e-gg-xx-v/viewer (Дата обращения: 15.04.2020).

[4] Медин А., Маринин С. Силы кибероперацій ВМС США и основные направления их применения // Pentagonus.URL: http://pentagonus.ru/publ/sily_kiberoperacij_vms_ssha_i_osnovnye_napravlenija_ikh_primenenija_2012/26-1-0-2268. (Дата обращения:26.04.2020).

[5] Горбачев Ю. Подготовка ВВС США к кибероперациям. // Pentagonus. URL: http://pentagonus.ru/publ/podgotovka_vvs_ssha_k_kiberoperacijam/13-1-0-1719. (Дата обращения: 27.04.2020).

[6] Ализар А. Киберкомандование США нанесло удар по Ирану // Хабр. URL: https://habr.com/ru/news/t/457376/. (Дата обращения: 07.04.2020).

[7] Васенин В.А. Информационная безопасность и компьютерный терроризм // Научные и методологические проблемы информационной безопасности (под ред. В.П.Шерстока, М.,МЦНМО, 2004).URL: https://http://docplayer.ru/30825002-Informacionnaya-bezopasnost-i-kompyuternyy-terrorizm-v-a-vasenin.html.(Дата обращения: 07.04.2020).

[8] Николаева А.Б., Тумбинская М.В. Киберпреступность: история развития, проблемы практики расследования// Виртуальный компьютерный музей. URL:https://computer-museum.ru/articles/materialy-mezhdunarodnoy-konferentsii-sorucom-2014/629/. (Дата обращения: 08.04.2020).

в изучение данных вопросов ценный вклад внесли Ш. Харрис[9], Дж. Адамс[10], Э. Клапес[11], С. Гош и Э. Туррини[12], Пол Ван Шаунбао и Р. Ледли[13], Е.Чабров[14], Дж.Линч[15]

Объектом исследования является государственная политика США в киберпространстве.

Предметом выступают наступательные и оборонительные стратегии, разрабатываемые и осуществляемые руководством США в киберпространстве, а также институциональные механизмы реализации этих стратегий.

Цель исследования состоит в анализе политики США в киберпространстве.

Задачи:

- изучить процесс закрепления и оформления основных целей и направлений американской киберполитики в стратегических документах, сопоставив официальную позицию по указанным вопросам в периоды президентства Б. Клинтона, Дж. Буша-мл., Б. Обамы и Д. Трампа;

- рассмотреть историю создания, организационную структуру и приоритетные цели деятельности основного государственного института

---

[9] Харрис Ш. Кибервойн@: Пятый театр военных действий/А. Никольский М.:Альпинанон-фикшн, 2016.

[10] Adams J. The Next World War. Computers Are the Weapons and the Front Line Is Everywhere. New-York, 1998.P. 55.

[11] [11]Clapes, A. Softwars : the legal battles for control of the global software industry. Westport, Conn.: Quorum Books, 1993. 53p.

[12] Ghosh S., Turrini E. Cybercrimes: A Multidisciplinary Analysis. Springer, 2010. p. 45-72.

[13] Wang S., Ledley R. Computer Architecture and Security: Fundamentals of Designing Secure Computer System // Wiley. URL:https://www.wiley.com/enus/Computer+Architecture+and+Security%3A+Fundamentals+of+Designing+Secure+Computer+Systems-p-9781118168813 P.133 (Дата обращения: 08.04.2020).

[14] Chabrow E. Military Mulls Joint Cyber Defense.//Gov Info Security. URL:http://www.govinfosecurity.com/articles.php?art_id=1450&search_keyword=Keith+Alexander&search_method=exact(Дата обращения: 26.04.2020).

[15] Lynch J. Cyber Command wants to partner with private sector to stop hacks // Fifth Domain. URL:https://www.fifthdomain.com/dod/cybercom/2018/07/31/cyber-command-wants-to-partner-with-private-sector-to-stop-hacks/ (Дата обращения: 07.04.2020).

обеспечения американской кибербезопасности – Киберкомандования США, а также специфику его взаимодействия с Министерством обороны США.

Источниковая база исследования. В рамках обозначенной темы в данном исследовании прорабатывались, в основном, официальные документы. В целях изучения политики Б.Клинтона относительно информационного пространства использовались Стратегия взаимодействия и расширения национальной безопасности(1995 г.)[16] и Стратегия национальной безопасности для нового века (1997 г.)[17]. Для проведения анализа киберполитики США при Дж. Буше-мл. были рассмотрены Национальная стратегия по безопасному киберпространству 2003г.[18] и Директива президента по национальной безопасности №54/Директива президента по внутренней безопасности №23[19]. Всеобъемлющая инициатива по обеспечению кибербезопасности[20], Международная стратегия по киберпространству 2011г.[21] и Стратегия кибербезопасности Министерства Обороны США 2015г .[22] помогли в изучении киберполитики Б. Обамы. Для

---

[16] A National Security Strategy of Engagement and Enlargement, February 1995// Historical Office of the Secretary of Defense. URL:https://history.defense.gov/Portals/70/Documents/nss/nss1995.pdf?ver=2014-06-25-121226-437 (Дата обращения: 08.04.2020).

[17] A National Security Strategy for a New Century, May 1997 //Historical Office of the Secretary of Defense. URL:https://history.defense.gov/Portals/70/Documents/nss/nss1997.pdf?ver=2014-06-25-121242-623 (Дата обращения: 08.04.2020).

[18] National strategy to secure cyberspace, February, 2003.[// Department of Homeland Security. URL:https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (Дата обращения: 09.04.2020).

[19] National security Presidential Directive NSPD-54/Homeland Security presidential directive HSPD-23, January 8, 2008 // Federation of American Scientists. URL:https://fas.org/irp/offdocs/nspd/nspd-54.pdf (Дата обращения: 10.04.2020).

[20] The Comprehensive National Cybersecurity Initiative // The White House President Barack Obama. URL:https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative (Дата обращения: 10.04.2020).

[21] The U.S. International Strategy for cyberspace, The White House, May 2011. // The White House President Barack Obama. URL:https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf(Дата обращения: 20.04.2020).

[22] The Department of Defense Cyber strategy, April 2015//U.S/ Department of Defense Archive. URL:https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf (Дата обращения: 20.04.2020).

того чтобы грамотно и эффективно оценить кибертактику Д. Трампа использовались Директива об усилении кибербезопасности федеральных сетей и критической инфраструктуры США 2017г.[23], Стратегия национальной безопасности США 2017г.[24], Национальная стратегия кибербезопасности США 2018г.[25]. Изучение организационной структуры и целей функционирования Киберкомандования США проводилось на основании Резюмирующей Киберстратегии Министерства Обороны США 2018г.[26]. Анализ совместной практической деятельности Киберкомандования и Министерства Обороны США проводился на основании информации, представленной новостными источниками Russia Today[27] и РБК[28].

Данная выпускная квалификационная работа состоит из введения, двух глав, первая из которых включает три раздела, а вторая -два раздела, заключения, списка источников и литературы.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В главе 1. *«Киберпространство в политике США»* рассматривается процесс становления и эволюция вопроса обеспечения сначала информационной, затем кибернетической безопасности США в условиях президентства Б. Клинтона, Дж. Буша –мл., Б. Обамы и Д. Трампа.

---

[23] Presidential Executive Order on Strengthening the Cyber security of Federal Networks and Critical Infrastructure. May 11, 2017. // The White House. URL:https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (Дата обращения: 25.04.2020).

[24] National Security Strategy. December 2017. // Homeland Security Digital Library. URL: https://www.hsdl.org/?abstract&did=806478 (Дата обращения: 25.04.2020).

[25] National Cyber Strategy of the United States of America, September 2018 // The White House. URL:https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (Дата обращения: 25.04.2020).

[26] Summary Department of Defense Cyber Strategy 2018 // U.S. Department of Defense. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (Дата обращения: 15.04.2020).

[27] Трамп выделил киберкомандование США в отдельную структуру. RT // Russia Today. URL:https://russian.rt.com/world/news/420622-kiberkomandovanie-otdelno-tramp 18.09.2017 (Дата обращения: 20.04.2020).

[28] Глава Пентагона объявил о начале кибервойны против ИГ РБК 06.04.2016 // РБК. URL:https://www.rbc.ru/politics/06/04/2016/5704e66d9a7947ceb004e0fc (Дата обращения: 07.04.2020).

В первой половине 1990 – х гг. происходило бурное развитие сети интернет, большинство пользователей которого являлись гражданами Соединенных Штатов Америки. На те же годы приходилось резкое повышение уровня активности хакерского сообщества в США. От «взломов» начали страдать не только рядовые пользователи, но и крупнейшие компании и даже правительственные компьютеры. Б.Клинтон стал первым президентом США, который начал задумываться о том, что безопасность компьютерных сетей должна официально входить список объектов национальной безопасности, которые могут быть подвержены угрозе. Поэтому администрация Б.Клинтона начала разработку специальных концептуальных документов, где информационное пространство упоминалось как цель для защиты. Дж. Буш-мл. продолжил тактику своего предшественника и именно он стал первым президентом в истории США, выпустившим официальный программный документ, полностью, посвященный кибербезопасности. Тогда же в законотворческий дискурс американских официальных лиц начали входить новые термины: «киберпространство», «кибербезопасность» и «киберугрозы». Также, именно Дж. Буш-мл. положил начало идее осуществления упреждающей киберполитики и проведению Соединенными Штатами превентивных операций в киберпространстве.

Следующий президент США построил свою кибеполитику на основании фундамента, который был заложен Б. Клинтоном и Дж. Бушем-мл.. Б. Обама стал первым американским президентом, который, несмотря на мнение американского истеблишмента, стал проводить политику международного сотрудничества в вопросах кибербезопасности. В его время был разработан ряд документов по международной кибербезопасности, а также были приняты специальные меры по совместной многосторонней работе. Б. Обамой было определено главное государственное ведомство, в компетенции которого находился вопрос кибербезопасность США. Им стало Министерство обороны США. Наряду с этим, все документы и механизмы в

области киберпространства, разработанные Б. Обамой за два его президентских срока, были направлены на достижение тех целей, которые были установлены еще его предшественниками. Данные цели включали в себя: защиту критической инфраструктуры; достижение технологический превосходства США в мире; наращивание кибервооружения; превентивную политику в киберпространстве; отстаивание и продвижение американских национальных интересов любыми средствами, в том числе, используя информационные сети и киберсферу.

Кибертактика же сегодняшнего президента США -Д.Трампа немногим отличаются от программ предыдущих президентов. Единственное новшество, привнесенное Трампом, заключается в том, что теперь за обеспечение кибербезопасности отвечают все органы исполнительной власти, а не только Министерство обороны США. Исходя из стратегий, принятых во время президентства Д.Трампа, основные черты киберполитики США остаются примерно такими же, какие существовали при Б. Обаме, Дж. Буше-мл. и Б. Клинтоне.

Глава 2. *«Институты и механизмы противостояния киберугрозам»* повествует о процессе создания и об организационной структуре Киберкомандования США, а также об основных целях и задачах совместной работы Киберкомандования и Министерства Обороны США.

В начале 2000-х гг. Министерство Обороны США официально признало, что кибернетическое пространство стоит военного внимания наравне с воздушным, водным, сухопутным и космическим. А уже к 2010г. было создано специальное военное подразделение, отвечающее напрямую за американскую кибербезопасность – Киберкомандование США.

Организационная структура Киберкомандования США комплексна и разнообразна. Она основана на киберсилах четырех отдельных военных подразделений США: Армии США, ВМС, ВВС и Корпуса морской пехоты. Каждый компонент имеет еще несколько подразделений в составе, где каждое ведомство обладает своими уникальными задачами.

Киберкомандование и Министерство Обороны посредством совместной деятельности осуществляют единую программу контроля американского киберпространства. Киберкомандование и Министерство имеют три основные цели: защита информационных систем Министерства Обороны; поддержка командований боевыми силами в киберпространстве и укрепление способности противостоять кибернетическим атакам на США. Задач гораздо больше, чем три. Сюда относится: достигнуть уровня кибервозможностей противников и превзойти его; сдерживание злонамеренной киберактивности; развитие устойчивости критической инфраструктуры; сотрудничество в киберсфере с частным сектором и международными партнерами; культивирование кибер-талантов и оптимизация структуры и функционала Министерства Обороны США.

ЗАКЛЮЧЕНИЕ

Становление и развитие киберполитики США началось в период президентства Б. Клинтона. Приставка «кибер» в тот период еще не употреблялась, и вместо нее использовалось понятие «информационное» пространство, нона президентство Б.Клинтона пришелся расцвет сети интернет, а вместе с ним и расцвет хакерской деятельности. Необходимо было срочно решать вопрос по регулированию процесса контроля и защиты американского информационного пространства. Именно поэтому Б.Клинтон считается первым президентом США, который начал рассматривать безопасность компьютерных сетей и всего информационного пространства в контексте национальной безопасности США. Клинтон впервые закрепил вопрос защиты информационного пространства в официальных документах. В это время информационное пространство и компьютерные сети были включены в критическую инфраструктуру США. Тогда же было положено начало сотрудничеству государства с частным сектором по вопросам информационной защиты критической инфраструктуры.

Понятия «кибернетический», а также «киберпространство», «киберугроза» вошли в политический лексикон во время президентских

сроков Дж. Буша-мл. Именно Дж. Буш-мл. положил начало тактике превентивной войны, в том числе, и в киберпространстве. Дж. Буш-мл. продолжил процесс укрепления киберзащиты критической инфраструктуры, но уже через отдельные государственные органы. Он стал первым президентом США, который разработал специальный документ, полностью посвященный кибербезопасности США.

Б. Обама, в отличие от своих предшественников, в своей киберполитической тактике сделал упор на международное сотрудничество в киберпространстве. При Б. Обаме были разработаны специальные документы, регулирующие международное киберсотрудничество; были определены основные области для межгосударственного совместной деятельности в кибероблсти. Помимо всего вышесказанного, во время президентских сроков Б. Обамы Министерство Обороны США начало самостоятельно разрабатывать специальные программные документы по обеспечению кибербезопасности США.

Д.Трамп из-за скандальных выборов 2016 включил институт выборов в критическую инфраструктуру США, обеспечение кибербезопасности которой предельно важно для американского руководства. В целом, Д.Трамп продолжает осуществление киберинициатив своих предшественников. Однако администрация Д.Трампа предпочитает двусторонние соглашения международным организациям. При Д.Трампе документально определяются официальные противники США в киберпространстве. В отношении них руководство Д.Трампа допускает проведение наступательных операций в киберпространстве, которые могут быть инициированы американской стороной.

Для реализации всех вышеупомянутых планов и стратегий Министерством Обороны США был создан специальный орган -Киберкомандование США. Главная роль Киберкомандования – это объединение кибер-сил, всех, по возможности, боевых подразделений США. Министерство Обороны, подведомственное ему Кибернетическое

Командование вместе с другими федеральными органами США имеют общую цель: достижение превосходства США и защита и продвижение американских национальных интересов. Что касается конкретной только лишь для этого ведомства цели, то Киберкомандование играет главную роль в обеспечении безопасности информационных сетей Министерства Обороны. Помимо этого, одной из главных задач совместной деятельности Министерства Обороны и Киберкомандования США является повышение уровня заинтересованности населения в феномене киберсферы. По мнению экспертов, повышение уровня кибеграмотности населения выступает главным гарантом успешной кибердеятельности США.