Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра международных отношений
и внешней политики России

ПРОБЛЕМА КИБЕРБЕЗОПАСНОСТИ ВО ВНЕШНЕПОЛИТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ АДМИНИСТРАЦИИ БАРАКА ОБАМЫ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

Студентки 4 курса 441 группы

направления 41.03.05 «Международные отношения»

Института истории и международных отношений

Ляпиной Алены Андреевны

Научный руководитель
доцент,
кандидат исторических наук _____ Д.С. Алексеев
подпись, дата

Зав. кафедрой
профессор,
доктор исторических наук _____ Ю.Г. Голуб
подпись, дата

Саратов 2018

Актуальность темы исследования. Несомненно, нарастающий интерес к проблемам обеспечения кибербезопасности значительно связан с активным участием США в вопросах, касающихся киберпространства.

Интернет и информационные технологии — достижения человечества, в основе которых лежит принцип доступности и открытости. Именно поэтому, будучи самой развитой страной с точки зрения последних технологий, США стали и самой уязвимой в плане кибератак, взломов и угроз.

В своих стратегических доктринах Соединенные Штаты провозгласила киберпространство новым полем возможных боевых действий. Вопрос обеспечения кибербезопасности во внешнеполитических и международно-договорных аспектах особенно сильно привлекал внимание правительства в период президентства Барака Обамы.

Раньше, все, что касалось проблем кибербезопасности, относили в основном к технологической стороне вопроса, особенно в отечественной историографии. С момента увеличения роли кибербезопасности в политических процессах США при 44-м президенте, выросла и потребность в исследованиях по данному вопросу в контексте внешней политики.

Цель данной работы состоит в анализе внешнеполитической деятельности администрации Б. Обамы в сфере кибербезопасности, а также ее влияния на современные международные отношения и положение США в мире.

Для достижения указанной цели предполагается решить следующие **задачи**:

- рассмотреть роль проблемы кибербезопасности во внешнеполитической повестке дня правительства США до избрания Б. Обамы;
- проанализировать политику обеспечения национальной кибербезопасности США в период президентства Барака Обамы;

- проанализировать совместную работу США с другими акторами международных отношений по разработке международных норм поведения в киберпространстве;
- рассмотреть взаимодействие США с союзниками по данной проблеме;
- на основе изученной информации определить степень эффективности и перспективы влияния политики при администрации Б. Обамы на кибербезопасность США.

Историография. Из-за актуальности проблематики было написано значительное количество исследовательской литературы, поэтому при написании квалификационной работы были прочитаны и проанализированы исследования отечественных и зарубежных ученых.

Среди отечественных исследователей особое внимание стоит обратить на работы Е. В. Батуевой[1], П.А. Шарикова[2] и П.А.Карасева[3]. О роли Соединенных Штатов в обеспечении кибербезопасности через принятие международно-правовых норм интерес представляют труды А.С. Алпеева[4], А.В Бедрицкого[5], О.В. Демидова и М.Б. Касеновой[6], а также Ю.В. Бородакия, А.Ю. Добродеева и И.В. Бутусова[7].

---

[1] *Батуева Е.В.* Политика администрации Б. Обамы в области обеспечения информационной безопасности // Вестник МГИМО. 2010. №4. [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/politika-administratsii-b-obamy-v-oblasti-obespecheniya-informatsionnoy-bezopasnosti (Дата обращения: 21.05.2017)

[2] *Шариков П.А.* Американская региональная политика кибербезопасности, 2016. [Электронный ресурс]. – URL: http://www.rusus.ru/print.php?id=524 (Дата обращения: 21.05.2017)

[3] *Карасев П.А.* Новые информационные технологии во внешней политике США// Мировая экономика и международные отношения. 2014. № 5. С. 53-62

[4] *Алпеев А.С.* Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности №5(8) – 2014

[5] *Бедрицкий А.В.* Международные договорённости по киберпространству: возможен ли консенсус? [Электронный ресурс]. – URL: https://riss.ru/images/pdf/journal/2012/4/10_.pdf (Дата обращения: 21.05.2017)

[6] *Демидов О.В., Касенова М.Б.* Кибербезопасность и управление интернетом // Статут, Москва, 2013. [Электронный ресурс]. – URL: http://pircenter.org/media/content/files/12/13969745490.pdf (Дата обращения: 19.03.2017)

[7] *Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В.* Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 1) [Электронный

Среди зарубежных исследователей значительное внимание непосредственно на сотрудничество США с союзниками обращают в своих работах Дж. Льюис[8], М. Кавелти[9], П. Маргулиес[10], С. Кьеркегор[11], Дж. Голдсмита[12], а также М. Хэтэуэй[13].

Источники. Для решения поставленных задач была привлечена источниковая база, состоящая из различных официальных документов, законов, двусторонних и многосторонних соглашений, резолюций, коммюнике, выступления официальных лиц и декларации саммитов, а также различных СМИ (The New York Times, The Guardian, TheCitizenLab и т.д.).

В первую очередь, необходимо обратиться к основным официальным государственным документам, а именно к Международной стратегии по

ресурс]. – URL: http://cyberleninka.ru/article/n/kiberbezopasnost-kak-osnovnoy-faktor-natsionalnoy-i-mezhdunarodnoy-bezopasnosti-hh-veka-chast-1 (Дата обращения: 21.05.2017)

[8] *Lewis J.A.* Conflict and Negotiation in Cyberspace // Center for Strategic and International Studies, February 2013. [Электронный ресурс]. – URL: http://csis.org/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf (Дата обращения: 11.03.2018)

[9] *Cavelty M.D.* Cyber-Allies: Strengths and Weaknesses of NATO's Cyberdefense Posture // IP Global Edition 12, no. 3, 2012. С. 11-15. [Электронный ресурс]. – URL: https://www.researchgate.net/publication/228199410_Cyber-Allies_Strengths_and_Weaknesses_of_NATO%27s_Cyberdefense_Posture (Дата обращения: 11.03.2018)

[10] *Margulies P.* Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy // Roger Williams University School of Law - 23.01.2017. [Электронный ресурс]. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2902212 (Дата обращения: 15.04.2017)

10. *Deibert R.* The Geopolitics of Cyberspace After Snowden // Current History 114, no. 768, 2015. С. 9-15. [Электронный ресурс]. – URL: http://www.currenthistory.com/Deibert_CurrentHistory.pdf (Дата обращения: 11.03.2018)

[11] *Kierkegaard S.M.* Cyber Law: Security and Privacy // Baro Association, Ankara, 2007. С.12

[12] *Goldsmith J.* Cybersecurity: A Skeptical View // Future Challenges in National Security and Law, edited by Peter Berkowitz. (2013). [Электронный ресурс]. – URL: http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf (Дата обращения: 11.03.2018)

[13] *Hathaway M.E.* Strategic Advantage: Why America Should Care About Cybersecurity // Belfer Center for Science and International Affairs, October 2009. [Электронный ресурс]. – URL: http://belfercenter.ksg.harvard.edu/files/Hathaway.Strategic%20Advantage.Why%20America%20Should%20Care%20About%20Cybersecurity.pdf (Дата обращения: 11.03.2018)

киберпространству[14], Стратегии международной кибербезопасности Госдепартамента США[15], Стратегии кибербезопасности Министерства Обороны США[16], Обзору политики в киберпространстве[17], к словарям основных военных терминов Министерства Обороны США за 2007[18] и 2017[19] годы, а также к выступлениям правительственных должностных лиц, например, речи Б. Обамы[20] или директора, отвечающего за информационную безопасность[21], а также официальные заявления администрации президента[22].

При изучении сотрудничества США с различными международными акторами Стратегия национальной безопасности Великобритании 2010г.[23],

[14] International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World // The White House, May 2011, C. 8. [Электронный ресурс]. – URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Дата обращения: 16.03.2017)

[15] Department of State International Cyberspace Policy Strategy // March 2016. [Электронный ресурс]. – URL: https://www.state.gov/documents/organization/255732.pdf (Дата обращения: 12.04.2018)

[16] Стратегия кибербезопасности Министерства Обороны США // Министерства Обороны США, апрель 2015 года. [Электронный ресурс]. – URL: https://defence.ru/document/61/ (Дата обращения: 25.04.2017)

[17] Cyberspace Policy Review // Official website of the Department of Homeland Security, 2009. [Электронный ресурс]. – URL: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf (Дата обращения: 13.03.2017)

[18]Department of Defense Dictionary of Military and Associated Terms (As Amended Through 17 October 2007) // [Электронный ресурс]. – URL: https://marineparents.com/downloads/dod-terms.pdf (Дата обращения: 13.03.2017)

[19] Department of Defense Dictionary of Military and Associated Terms (As of March 2017) // [Электронный ресурс]. – URL: https://www.hsdl.org/?abstract&did=799027 (Дата обращения: 13.03.2017)

[20] Remarks by The President on Securing our Nation's Cyber Infrastructure // The White House, Office of the Press Secretary, – 29.05.2009. [Электронный ресурс]. – URL: https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (Дата обращения: 20.03.2018)

[21] *Wilshusen G.C., Powner D.A.* Continued Efforts Are Needed to Protect Information Systems from Evolving Threats // November 17, 2009. [Электронный ресурс]. – URL: https://www.gao.gov/new.items/d10230t.pdf (Дата обращения: 30.03.2018)

[22] US Department of State, "U.S. Intervention at the World Conference in International Telecommunications", Washington DC, Media Note, 13 December 2012.

[23] A Strong Britain in an Age of Uncertainty: The National Security Strategy // Октябрь 2010 г. [Электронный ресурс]. – URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf (Дата обращения: 12.04.2018)

двустороннее коммюнике между США и Великобританией 2011г.[24], совместное коммюнике США и Канады 2011 г.[25]

Среди документов международных организаций: Руководство по национальной кибербезопасности[26] для Международного Союза Электросвязи, официальный документ ЕС "Стратегия кибербезопасности Европейского Союза: открытое, безопасное и надежное киберпространство"[27], а также основные моменты кибербезопасности НАТО[28], декларации саммитов Альянса, которые проходили в 2010г.[29] и 2014г.[30] Важной вехой в развитии кибербезопасности НАТО стало признание киберпространства возможной зоной ведения войны[31].

Структура работы. Выпускная квалификационная работа состоит из введения, двух глав, а также заключения, списка использованных источников и литературы.

---

[24] US-UK Cyber Communiqué // 25.05.2011. [Электронный ресурс]. – URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62647/CyberCommunique-Final.pdf (Дата обращения: 05.04.2018)

[25] Unites States-Canada Beyond the Border. A shared version for perimeter security and economic competitiveness, December 2011

[26] *Wamala F.* ITU National Cybersecurity Guide // Geneva, 2011. [Электронный ресурс]. – URL: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf (Дата обращения: 15.03.2017)

[27] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace // JOIN(2013) 1 final – 07.02.2013. [Электронный ресурс]. – URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2013-0376+0+DOC+PDF+V0//EN (Дата обращения: 12.04.2018)

[28] Cyber Defense // Official Website of NATO. 19 Feb., 2018 . [Электронный ресурс]. – URL: http://www.nato.int/cps/en/natohq/topics_78170.htm (Дата обращения: 26.04.2018)

[29] Lisbon Summit Declaration // Официальный сайт НАТО, – 20.11.2010. [Электронный ресурс]. – URL: https://www.nato.int/cps/en/natohq/official_texts_68828.htm (Дата обращения: 20.03.2018)

[30] Wales Summit Declaration // Официальный сайт НАТО – 05.09.2014. [Электронный ресурс]. – URL: https://www.nato.int/cps/ic/natohq/official_texts_112964.htm (Дата обращения: 05.04.2018)

[31] Cyber Defense Pledge// Official Website of the US Mission to NATO. 8 July, 2016. [Электронный ресурс]. – URL: https://nato.usmission.gov/cyber-defense-pledge/?_ga=2.147978167.109758692.1526227682-873922072.1526227682 (Дата обращения: 26.04.2018)

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе «Эволюция роли киберпространства в обеспечении национальной безопасности США» рассматривается эволюция роли проблемы кибербезопасности в политической повестке дня США. Первый параграф «Проблема кибербезопасности в политической повестке дня США в начале XXI века» посвящен становлению вопроса кибербезопасности в национальной безопасности Соединенных Штатов. Изначально вопросы кибербезопасности с точки зрения внутренней и внешней политики разделялись между собой. Так, внутри страны принимались различные меры по укреплению информационной безопасности, противодействию криминалу и терроризму в данной области, активно разрабатывались новейшие технологий, сценарии информационных войн и операций для военного сектора страны. Но на внешнеполитическом поприще дела не обстояли столь хорошо, так как позиции США сводились долгое время только к тому, что угрозу в киберпространстве возникают лишь из-за неправомерных действий, а не в результате активности одних государств в отношении других. Таким образом, в связи с ускорением процессов глобализации, развитием информационно-коммуникационных технологии, а также с возникновением новых угроз международной безопасности, возникла необходимость в расширении политического курса США не только по вопросу национальной кибербезопасности, но и в отношении международного сотрудничества по данному вопросу.

Во втором параграфе «Изменение методов реализации стратегии кибербезопасности во время президентства Б. Обамы» говорится о непосредственных изменениях политики в отношении киберпространства, предпринятых Б. Обамой с момента вступления в должность. О значимости роли кибербезопасности в США стали масштабно говорить с начала первого президентства Б. Обамы. 29 мая 2009 года Б. Обама выступил с речью, в которой затронул планы его администрации для формирования нового комплексного подхода к обеспечению кибербезопасности инфраструктуры

Америки. США стремятся трансформировать глобальное информационное пространство в такую среду, которая позволит им беспрепятственно использовать ИКТ как инструменты реализации своих национальных интересов.

Материал **второй главы «Особенности сотрудничества администрации Б. Обамы с другими странами в сфере кибербезопасности»** посвящён внешнеполитической составляющей политики Б. Обамы в отношении киберпространства.

В первом параграфе «Разработка международных норм поведения в киберпространстве: реформирование глобальной системы управления Интернетом, Европейская Конвенция о борьбе с киберпреступлениями» рассматриваются международные противоречия, связанные с различными подходами к проблеме глобального управления информационным пространством, которые обострились в ходе попыток международного сообщества и в частности США реформировать существующую систему управления Интернетом. Во время Всемирной конференции по телекоммуникациям (WCIT), проводимой МСЭ (телекоммуникационным агентством ООН) и проведенной в Дубае в декабре 2012 года, Россия, Китай, Саудовская Аравия, Алжир и Судан представили резолюцию, в которой говорится, что государства-члены имеют право вмешиваться во все вопросы, касающиеся международного управления Интернетом. Документ был позже отозван, но Ассамблея одобрила (большинством голосов) необязательную для выполнения резолюцию.

В итоге, несмотря на стремление США участвовать в формировании международных норм поведения в киберпространстве, нежелание американского правительства идти на уступки из-за различия интересов с такими странами как Китай и Россия, оставило ряд вопросов неразрешенными, или же привело к отказу ряда стран подписать совместное соглашение, как это произошло с конвенцией о борьбе с киберпреступлениями.

Во втором параграфе «Совместная работа США, НАТО и ЕС в вопросах обеспечения кибербезопасности» рассматривается проблема сотрудничества Соединенных Штатов с международными организациями по вопросу кибербезопасности. Способность США реагировать на внешние киберугрозы и бороться с транснациональной киберпреступностью значительно усиливается, благодаря возможностям их международных партнеров в этой области. Поэтому Госдепартамент США работает с различными департаментами, агентствами, союзниками и другими партнерами в целях укрепления потенциала иностранных правительств, особенно в развивающихся странах, для обеспечения своих собственных сетей, а также для расследования и преследования киберпреступников в пределах их границ. Департамент также активно содействует сотрудничеству по совместному наращиванию кибернетического потенциала. С началом работы администрации Б. Обамы значительно вырос интерес в сотрудничестве с Европейским союзом и НАТО, в первую очередь в технологической сфере.

Несмотря на очевидную возможность для продолжения сотрудничества и даже перспективы для создания своеобразной коллективной кибербезопасности НАТО, в новой стратегии кибербезопасности США, опубликованной министерством обороны страны, ни НАТО, ни ЕС не рассматриваются в качестве стратегических партнеров по обеспечению безопасности в киберпространстве. В документе Соединенные Штаты подчеркивают важность кооперации с Канадой, Великобританией, Австралией, а также с союзниками на Ближнем Востоке, в Азиатско-Тихоокеанском регионе и с некоторыми ключевыми действующими акторами в самом Альянсе.

Наконец, в третьем параграфе «Особенности двустороннего сотрудничества США с союзниками в сфере кибербезопасности» речь идет о стремлении администрации Б. Обамы расширить возможности Соединенных Штатов в области международной кибербезопасности через двустороннее

сотрудничество со странами-союзниками. Помимо борьбы с киберпреступностью, США и их ближайшие союзники также должны работать вместе, чтобы понизить свою уязвимость и сократить последствия успешной кибератаки. Но со многими союзниками США тесное сотрудничество в области кибербезопасности начинается со стремлений восстановить доверие и технологическое взаимодействие, в то время как до налаживания совместной политики и стратегии в киберпространстве даже не доходит. Наибольших успехов администрации Б. Обамы удалось добиться в достижении различных соглашений, направленных, в первую очередь, на техническую модернизацию, с Великобританией, Канадой и Австралией, а также на научно-исследовательскую деятельность совместно с Израилем.

Кроме того, вслед за скандалом с Эдвардом Сноуденом мир обратился к США за ответами на вопросы, касающиеся наблюдения и конфиденциальности, требования скоординированного ответа на растущее число случаев глобального взлома преступниками и государствами-изгоями. Для одних государств-единомышленников кибербезопасность оставалась новой неизведанной областью, и им не хватало технологического развития, для других же, киберпространство являлось новой возможностью реализации экономического потенциала, но точно не военного.

ЗАКЛЮЧЕНИЕ

Практически все аспекты кибербезопасности имеют транснациональный компонент, влияющий на пользователей киберсистем во всем мире. Тем не менее, усилия правительства США по предотвращению кибератак и эксплуатации, хотя формально выступают за международное сотрудничество, основаны почти исключительно на односторонних мерах.

Поэтому с 2009 года в США формируется особая политика по обеспечению кибербезопасности. Во-первых, продолжается работа над совершенствованием национальной кибербезопасности, а за счет госбюджета улучшаются информационные технологии. Во-вторых, в целях сохранения американского преимущества в киберпространстве, все международные инициативы по созданию любых правовых норм, которые бы ограничивали эти достижения США, никогда не реализуются, довольствуясь неэффективными соглашениями. В-третьих, двустороннее партнерство Соединенных Штатов с союзниками оказалось гораздо продуктивнее, чем международно-правовая активность.

При этом сотрудничество в рамках НАТО ограничилось вступлением США в Объединенный центр передовых технологий и кибероборонь в 2011 году. Инициатива в Альянсе по этому вопросу, в первую очередь, осталась за Прибалтийскими государствами.

При формировании политики в области кибербезопасности администрация президента Барака Обамы столкнулась с серьезными препятствиями. Первым серьезным препятствием было нежелание Конгресса принять всеобъемлющее законодательство. Вторым препятствием, особенно после откровений Эдварда Сноудена о наблюдении спецслужб США в 2013 году, был международный дефицит доверия. Все это стало проблемой для формирования четкой глобальной позиции Соединенных Штатов, поскольку такие вопросы, как кибербезопасность и разведка, имеют международные последствия. Например, наблюдение США за жителями иностранных государств может повлиять на право на неприкосновенность частной жизни,

установленные транснациональными соглашениями. Более того, запросы правоохранительных органов о данных могут влиять на программное обеспечение и связанные с Интернетом услуги, которые являются международными по своим масштабам и охвату.

В центре наследия Б. Обамы будет совместная работа государственного и частного сектора на добровольной основе для оценки рисков в сфере кибербезопасности. Национальный институт стандартов и технологий курировал разработку рамочного соглашения после распоряжения президента Б. Обамы в 2013 году. Должностные лица администрации промоутировали принятие данного соглашения в частном секторе США и продвигали его в качестве модели для других стран. Тем не менее, некоторые в промышленности говорят, что внедрение этой структуры замедлилось из-за отсутствия четких данных об ее экономической эффективности. А в Европейском союзе к данным мерам отнеслись скептично, упрекая правительство США в недостаточной защите личных данных физических лиц.

Таким образом, за два президентских срока Барака Обамы, политика США в киберпространстве стала важным фактором американской внешней политики. Национальные интересы США в этой сфере реализуются на нескольких направлениях, прежде всего, через активное влияние на процесс формирования глобального информационного пространства и его нормативно-правовое регулирование, участие в развитии ИКТ своих союзников для обеспечения собственной национальной безопасности и сохранения своих позиций в мире.