На правах рукописи

Батуева Елена Владимировна

АМЕРИКАНСКАЯ КОНЦЕПЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЕЕ МЕЖДУНАРОДНО-ПОЛИТИЧЕСКАЯ СОСТАВЛЯЮЩАЯ

Специальность: 23.00.04 – политические проблемы международных отношений, глобального и регионального развития

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата политических наук

Москва – 2014

Работа выполнена на кафедре мировых политических процессов Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации».

Научный руководитель: **КРУТСКИХ Андрей Владимирович**
доктор исторических наук, профессор

Официальные оппоненты: **АБРАМОВА Ольга Дмитриевна**
доктор политических наук, профессор, заведующая кафедрой внешнеполитической деятельности России Российской академии народного хозяйства и государственной службы при Президенте РФ

РОГОВСКИЙ Евгений Александрович
кандидат экономических наук, руководитель Центра проблем военно-промышленной политики Института США и Канады РАН

Ведущая организация: **Московский государственный университет им. М.В. Ломоносова**

Защита состоится « 19 » января 2015 г. в «14.00» часов в аудитории ____ на заседании Диссертационного совета Д 209.002.02 (политические науки) при Московском государственном институте международных отношений (Университете) МИД России по адресу: 119454 Москва, проспект Вернадского, дом 76.

С диссертацией и авторефератом можно ознакомиться в научной библиотеке им. И.Г. Тюлина МГИМО (У) МИД России по адресу: 119454, г. Москва, проспект Вернадского, 76 и на сайте www.mgimo.ru.

Автореферат разослан «….» …… 2014 г.

Ученый секретарь
Диссертационного совета к.полит.н. Истомин И.А.

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Информационно-коммуникационные технологии (ИКТ) глубоко проникли во все сферы жизнедеятельности государства и общества, которые все больше зависят от стабильного функционирования информационной инфраструктуры. В свою очередь, информационно-коммуникационные системы и сети становятся объектом злонамеренных действий со стороны большого числа акторов. В этой связи вопросы информационной безопасности являются одним из важных направлений обеспечения национальной безопасности всех технологически развитых стран.

Сегодня борьба за обладание информацией, достижение и удержание информационного превосходства занимает значительное место в геополитической конкуренции стран. Государства, развивающие потенциал в информационном пространстве, получают целый ряд конкурентных преимуществ и могут использовать его как фактор силы в ущерб интересам остальных участников международных процессов. В этой связи особую актуальность приобретают вопросы использования ИКТ государствами в военно-политических целях.

Такие характеристики информационного пространства, как трансграничность, открытость, доступность и анонимность обусловили привлекательность информационной инфраструктуры с точки зрения возможности осуществления неправомерных действий в преступных и террористических целях. Противодействие данным видам угроз становится важной составляющей комплекса мер по обеспечению информационной безопасности как на национальном, так и на глобальном уровне.

США являются одним из ключевых игроков на международной арене, лидерами в области ИКТ, страной, где зародилась всемирная глобальная сеть Интернет. При этом технологический прогресс, с одной стороны, способствовал укреплению роли США как глобального лидера, с другой – стирание барьера географического расстояния, сетезависимость, рост числа

средств и методов осуществления информационных атак резко повысили степень уязвимости страны. В этой связи США одними из первых начали разработку стратегии по обеспечению безопасности в киберпространстве, изучение которой представляет как научный, так и практический интерес.

Рассмотрение американского видения информационных угроз и их подхода к обеспечению информационной безопасности представляется важным и необходимым в силу того, что киберполитика Соединенных Штатов оказывает непосредственное влияние на состояние безопасности отдельных стран и международной стабильности и безопасности в целом.

Постоянно обновляемые национальные стратегии, военные концепции и доктрины демонстрируют эволюцию в подходах руководства США и формируют тенденции в области использования ИКТ в военно-политических целях. Опыт США по обеспечению безопасности критической инфраструктуры страны, 85% которой принадлежит частному сектору, также является уникальным. Процесс формирования правовых механизмов обеспечения информационной безопасности в США, с одной стороны, демонстрирует сложность и комплексность этих вопросов, с другой – потенциальные направления развития нормотворчества в данной области. Кроме того, США во многом задают вектор международной дискуссии, являясь одним из ключевых участников переговорного процесса по вопросам международной информационной безопасности (МИБ) [1].

Степень научной разработанности проблемы. ИКТ оказали существенное воздействие на цивилизационное развитие и глобальные процессы, затронув все сферы жизнедеятельности общества и государства. В связи с этим существенно возрос интерес научного сообщества к изучению последствий информатизации. При написании диссертации автор опирался

[1]Под международной информационной безопасностью понимается такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры. См. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года от 24 июля 2013 г. [Электронный ресурс]. –URL: http://www.scrf.gov.ru/documents/6/114.html (дата обращения: 05.04.14).

как на теоретические работы, так и на эмпирические исследования зарубежных (в первую очередь американских) и российских авторов по широкому спектру вопросов, связанных с обеспечением информационной безопасности.

В 1970-х годах начала формироваться теория информационного общества как новый этап развития постиндустриального общества. Работы Д. Бэлла[2], М. Кастельса[3], Й. Масуды[4] и М. Пората[5] заложили основу концепции информационного общества и определили его основные характеристики.

Последствия трансформации общества и государства под влиянием ИКТ, а также их воздействие на политические процессы на национальном и международном уровне рассмотрены в работах зарубежных исследователей У. Бека[6], Дж. Коэна[7], М. Мура[8], Дж. Ная мл.[9], Дж. Розенау[10], А. Тоффлера[11], Т. Фридмана[12], Ф. Фукуямы[13], Э. Шмидта и др., а также российских

[2] Bell D. The Social Framework of the Information Society / Eds. Michael L. Dertouzous, J. Moses (eds) // The Computer Age: A 20 Year View, Cambridge, MA: MIT Press, 1980. – P. 163-212; Bell D. The Third Technological Revolution and Its Possible Socioeconomic Consequences / Daniel Bell // Dissent, – 1989. – 6 (2). – P. 164-176; Bell D. The Coming of Post-Industrial Society: A Venture in Social Forecasting. / Daniel Bell. – New York: Basic Books, 1999. – 616 p.

[3] Castells M. The rise of the network society / Manuel Castells. – Malden, Mass.: Blackwell Publishers, 1996. – 556 p.

[4] Masuda Y. The information Society as Post-Industial Society / Yoneji Masuda. – Washington, 1981. – 179 p.

[5] Porat M. The Information Economy: Development and Measurement / M. Porat, M Rubin. – Washington, 1978. – 320 p.

[6] Бек У. Что такое глобализация? / У. Бек. – М., 2001. – 289 с.

[7] Шмидт Э. Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государств / Эрик Шмидт, Джаред Коэн; пер. с англ. С. Филина. – М.: Манн, Иванов и Фербер, 2013. – 368 с.

[8] Moore M. Saving Globalization: Why Globalization and Democracy Offer the Best Hope for Progress, Peace and Development / Mike Moore. – Hoboken, NJ: John Wiley & Sons (Asia), 2009. – 293 p.

[9] Nye J. Power in the Global Information Age: From Realism to Globalization / Joseph S. Nye Jr. – Routledge, 2004. – 240 p.; Nye J. The Future of Power / Joseph S. Nye Jr. – New York: Public Affairs, 2011. – 298 p.

[10] Rosenau J. N. Turbulence in World Politics. A Theory of Change and Continuity / James N. Rosenau. - Princeton University Press, New Jersey, 1990. – 463 p.

[11] Тоффлер Э. Третья волна / Э. Тоффлер. – М.: АСТ, 2010. – 784 с.

[12] Friedman T. The Lexus and the Olive Tree: Understanding Globalization / Thomas L. Friedman. –New York: Farrar, Straus and Giroux, 1999. – 394 p.; Friedman T. The World is Flat: Brief History of the Twenty First Century / Thomas L. Friedman. – New York: Farrar, Straus and Giroux, 2007. – 660 p.

[13] Fukuyama, Francis. The Promise and Challenge of emerging technologies [Электронный ресурс] / Information and Biological Revolutions: Global Governance Challenge // Science and Technology Policy Institute. Chapter 2. – URL: http://www.rand.org/content/dam/rand/pubs/monograph_reports/2007/MR1139.pdf (дата обращения: 05.04.14).

исследователей – Д.Г. Балуева[14], О.Н. Вершинской[15], А.В. Крутских[16], М.М. Лебедевой[17], Д.Н. Пескова[18], А.В. Торкунова[19], П.А. Цыганкова[20] и др.

При изучении вопросов информационной безопасности США, включая ее международно-политическую составляющую, необходимо учитывать системообразующую роль Соединенных Штатов в международных отношениях и их глобальную стратегию, которые рассматриваются в работах известных российских авторов таких, как А.Г. Арбатов[21], Г.А. Арбатов[22], А.П. Барышев[23], А.Д. Богатуров[24], Ю.П. Давыдов[25], В.Л. Иноземцев[26], С.А. Караганов[27], В.А. Кременюк[28],

---

[14] Балуев Д.Г. Информационная революция и мировая политика / Под ред. М.М. Лебедевой // Методические материалы и программы к специализированным курсам по гуманитарным и социально-экономическим дисциплинам. – М.: Аспект-Пресс, 2002. С. 11-25.

[15] Вершинская О.Н. Адаптация общества к новым информационным технологиям: новые возможности и новое социальное неравенство / О.Н. Вершинская // Информационное общество. – 1999. – №1. – С. 25-29.

[16] Крутских А.В. Дипломатия и информационно-коммуникационная революция / А.В. Крутских, Г.Г. Крамаренко // Международная жизнь. – 2003. – № 7. – С. 111-112; Инновационные направления современных международных отношений / Учебное пособие для студентов вузов под ред. А.В. Крутских и А.В. Бирюкова. – Аспект Пресс, 2010. – 295 с.

[17] Лебедева М.М. Современные технологии и политическое развитие мира / М.М. Лебедева // Международная жизнь. – 2001. – № 2. – С. 45-53; Лебедева М.М. Мировая политика / М.М. Лебедева. – М.: Аспект Пресс, 2003. – 351 с.

[18] Песков Д.Н. Интернет в российской политике: утопия и реальность / Д.Н. Песков // Полис. – 2002. – №1. – С. 35-45.

[19] Современные международные отношения и мировая политика: Учебник/ А.В. Торкунов, И.Г. Тюлин, А.Ю. Мельвиль и др.; Моск. гос. ин-т междунар. отношений (Университет) МИД России. Отв. ред. А.В. Торкунов. – М.: Просвещение: МГИМО, 2004. – 991 с.

[20] Цыганков П.А. Теория международных отношений / П.А. Цыганков. – М.: Гардарика, 2005. – 590 с.

[21] Арбатов А.Г. Угрозы реальные и мнимые: Военная сила в мировой политике начала XXI века. [Электронный ресурс] // Россия в глобальной политике. 3 марта 2013 г. – URL: http://www.globalaffairs.ru/number/Ugrozy-realnye-i-mnimye-15863 (дата обращения: 05.04.14).

[22] Арбатов Г.А. Современная внешняя политика США: в двух томах / Г.А. Арбатов, Г.А. Трофименко. – М.: Наука, 1984.

[23] Барышев А.П. Современная стратегия США и НАТО / А.П. Барышев. – М.: ОГИ, 2011. – 248 с.

[24] Богатуров А.Д. «Стратегия перемалывания» в международных отношениях и внешней политике США / А.Д. Богатуров. – М.: Едиториал Урсс, 2004. – 48 с.; Богатуров А.Д. Глобальные аспекты «цивилизационного» влияния США в XXI в. / А.Д. Богатуров // Мировая экономика и международные отношения. – 2007. – № 9. – С. 114-122; Современная мировая политика. Прикладной анализ / Отв. ред. А.Д. Богатуров. – М.: Аспект-пресс, 2009. – 588 с.

[25] Давыдов Ю.П. Россия и США: после «холодной войны» / Ю.П. Давыдов, В.А. Кременюк. – М.: Наука, 1999. – 141 с.

[26] Иноземцев В.Л. О мировом порядке XXI века / В. Л. Иноземцев, С. А. Караганов // Россия в глобальной политике. – 2005. – № 1. – С. 8-26.

[27] Караганов С.А. XXI век: контуры миропорядка / С.А. Караганов // Россия в глобальной политике. – 2005. – № 5. – С. 36-50.

[28] Кременюк В.А. США и окружающий мир: уравнение со многими неизвестными / В.А. Кременюк // США-Канада: экономика, политика, культура. – 1999. – №1. – 5-19; Кременюк В.А. Две модели отношений США с окружающим миром: «заботливый отец» или «суровый шериф» / В.А. Кременюк // США-Канада: экономика, политика, культура. – 2004. – № 11. – С. 3-14.

В.М. Кулагин[29], В.О. Печатнов[30], Т.П. Подлесный[31], Е.М. Примаков[32], С.М. Рогов[33], А.И. Уткин[34], Т.А. Шаклеина[35] и др., а также таких ведущих американских экспертов, как Зб. Бжезинский[36], Ф. Закария[37], Г. Киссинджер[38], Дж. Най[39], Ф. Фукуяма[40], С. Хантингтон[41] и др.

Отдельного внимания заслуживают многочисленные работы американских исследователей, журналистов и политических деятелей, посвященные различным аспектам обеспечения национальной безопасности США, которые в том числе учитывают новый контекст безопасности, связанный с использованием потенциала ИКТ. Среди них можно выделить работы Дж. Голдсмита[42], Э. Картера[43], Р. Кларка и Р. Кнейка[44], Фр. Крамера,

[29] Кулагин В.М. Международная безопасность: Учебное пособие для студентов вузов / В.М. Кулагин. – М.: Аспект Пресс, 2006. – 319 с.
[30] Печатнов В.О. История внешней политики США / В.О. Печатнов, А.С. Маныкин. – М.: Международные отношения, 2012. – 688 с.
[31] Подлесный Т.П. Политика США в меняющемся мире / Т.П. Подлесный, В.И. Батюк. – М.: Наука, 2004. – 332 с.
[32] Примаков Е.М. Мир после 11 сентября / Е.М. Примаков. – М.: Мысль, 2002. – 190 с.; Примаков Е.М. Мир без сверхдержав / Е.М. Примаков // Россия в глобальной политике. – 2003. – № 3. – С. 80-85; Примаков Е.М. Мысли вслух / Е.М. Примаков. – М.: Российская газета, 2011. – 207 с.
[33] Рогов С.М. США на рубеже веков / С.М. Рогов. – М.: Наука, 2000. – 495 с.; Рогов С.М. 11 сентября 2001 года: Реакция США и последствия для российско-американских отношений / С.М. Рогов. – М., ИСКРАН, 2001. – 88 с.; Рогов С. М. Доктрина Буша / С.М. Рогов // Свободная мысль - XXI. – 2002. – № 4. – С. 4-14.
[34] Уткин А.И. Стратегия США для XXI века / А.И. Уткин // США-Канада: экономика, политика, культура. – 1999. – № 7. – С. 17-28.
[35] Шаклеина Т.А. Россия и США в мировой политике: Учеб. Пособие для студентов вузов / Т.А. Шаклеина. – М.: Аспект Пресс, 2012. – 272 с.
[36] Бжезинский Зб. Великая шахматная доска / Зб. Бжезинский, пер. О.Ю. Уральской. – М.: Международные отношения, 1998. – 256 с.; Бжезинский Зб. Выбор. Мировое господство или глобальное лидерство / Зб. Бжезинский. – М.: Международные отношения, 2004. – 287 с.; Бжезинский Зб. Ещё один шанс. Три президента и кризис американской сверхдержавы / Зб. Бжезинский. – М: Международные отношения, 2010. – 190 с.;
[37] Zakaria F. The Post-American World / Fareed Zakaria. – New York: W.W. Norton, 2009. – 292 p.
[38] Киссинджер Г. Дипломатия. / пер. с англ. В.В. Львова. – М.: Ладомир, 1997. – 848 с.; Kissinger H. Does America Need a Foreign Policy?: Toward a Diplomacy for the 21st Century / Henry A. Kissinger. – New York: Simon & Schuster, 2001. – 238 p.
[39] Nye J. The Future of American Power: Dominance and Decline in Perspective / Joseph S. Nye, Jr. // Foreign Affairs. Nov. / Dec. 2010. V. 89. #6. – P. 2-12.
[40] Fukuyama Fr. America at the Crossroads: Democracy, Power, and the Neoconservative Legacy / Francis Fukuyama. – Yale University Press, 2006. – 226 p.
[41] Huntington S. The Lonely Superpower / Samuel P. Huntington // Foreign Affairs. – March/April 1999. – Vol.78. № 2. – P. 35-49.
[42] Goldsmith J. Power and Constraint: The Accountable Presidency After 9/11 / Jack Goldsmith. – New York: W.W. Norton & Co., 2012. – 311 p.
[43] Carter A. Preventive Defense. A New Security Strategy for America / Ashton B. Carter, William J. Perry. – Washington, D.C.: Brookings Institution Press, 1999. – 256 p.
[44] Clarke R. Cyber War the Next Threat to National Security and What to Do About It / Richard A. Clarke and Robert K. Knake. – HarperCollins, 2010. – 290 p.

Т. Льюиса[45], Э. Накашимы[46], С. Реншона[47], П. Розенцвайга[48], Д. Санджера[49], П. Сингера[50], С. Старра, Л. Уэнтца[51], М. Хатауей[52], Э. Шмитта[53] и др.

В американском научном сообществе активная дискуссия по вопросам информационной безопасности ведется с конца 1970-х гг. Большое число теоретических и практических разработок американских авторов посвящено вопросам использования ИКТ в военно-политических целях – информационной войне, информационным операциям. В данном исследовании были использованы работы Дж. Аркуиллы[54], Д. Деннинг[55], М. Либики[56], Т. Рона[57], Д. Ронфельда, Т. Томаса[58], А. Тоффлера[59], К. Уилсона[60], С. Уинтерфельда[61] и У. Швартау[62].

---

[45] Lewis T. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation / Ted G. Lewis. – Hoboken, N.J.: Wiley-Interscience, 2006. – 474 p.

[46] Nakashima, Ellen. With Plan X, Pentagon seeks to spread U.S. military might to cyberspace [Электронный ресурс] // The Washington Post. May 30, 2012. – URL: http://articles.washingtonpost.com/2012-05-30/world/35458424_1_cyberwarfare-cyberspace-pentagon-agency (дата обращения: 05.04.14).

[47] Renshon St. National Security In the Obama Administration: Reassessing the Bush Doctrine / Stanley A. Renshon. – New York and London: Routledge, 2009. – 312 p.

[48] Rosenzweig P. Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World / Paul Rosenzweig. – Santa Barbara, Calif.: Praeger, 2013. – 290 p.

[49] Sanger D. The Inheritance. A New President Confronts the World / David E. Sanger. – Black Swan, 2009. – 513 p.; Sanger D. Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power / David E. Sanger. – New York: Broadway Paperbacks, 2012. – 485 p.

[50] Singer P.W. Cybersecurity and Cyberwar: What Everyone Needs to Know / Peter W. Singer, Allan Friedman. – OXFORD University Press, 2014. – 306 p.

[51] Cyberpower and National Security / Ed. by F. Kramer, S. Starr, L. Wentz. – Potomac Books Inc., 2009. – 664 p.; Military Perspectives on Cyberpower / Ed. by L. Wentz, C.Barry, S. Starr. – CreateSpace Independent Publishing Platform, 2012. – 128 p.

[52] Hathaway, Melissa. Strategic Advantage: Why America Should Care About Cybersecurity [Электронный ресурс] / Belfer Center for Science and International Affairs. October 2009. – URL: http://belfercenter.ksg.harvard.edu/files/Hathaway.Strategic%20Advantage.Why%20America%20Should%20Care%20About%20Cybersecurity.pdf (дата обращения: 05.04.14).

[53] Schmitt E. Counterstrike: the untold story of America's secret campaign against al Qaeda / Eric Schmitt and Thom Shanker. – New York: Times Books, 2011. – 324 p.

[54] In Athena's Camp: Preparing for Conflict in the Information Age [Электронный ресурс] / Ed. by John Arquilla, David Ronfeldt. – Santa Monica: RAND, 1997. – URL: http://www.rand.org/pubs/monograph_reports/MR880.html; Arquilla, John and Ronfeld, David. The Emergence of Neopolitik: Towards an American Information Strategy [Электронный ресурс] // RAND, 1999. http://www.rand.org/pubs/monograph_reports/MR1033.html (дата обращения: 05.04.14)

[55] Denning D. Information Warfare and Security / Dorothy E. Denning. – New York: ACM Press, 1999. – 522 p.

[56] Libicki M. What is Information Warfare? / Martin C. Libicki // The Center for Advanced Command Concepts and Technology. – 2005. – P.104; Libicki, Martin. Cyberdeterrence and Cyberwar [Электронный ресурс] // RAND, 2009. – 214 p. – URL: http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf; Libicki M. Cyberwar as a Confidence Game / Martin Libicki // Strategic Studies Quaterly. – Vol. 5. No.1. – Spring 2011. – P. 132-146.

[57] Rona, Thomas. Weapons Systems and Information War [Электронный ресурс] / Boeing Aerospace Company. Seattle, Washington. July 1976. – URL: http://www.dod.mil/pubs/foi/homeland_defense/missile_defense_agency/09-F-0070WeaponSystems_and_Information_War.pdf (дата обращения: 05.04.14)

Значимый вклад в исследование угроз информационной безопасности, их содержания и основных характеристик внесли российские исследователи В.А. Голубев[63], Е. Касперский[64], В.Н. Лопатин[65], Г.Л. Смолян[66], А.А. Стрельцов[67], А.В. Федоров[68], а также зарубежные – Р. Алдрих[69], Дж. Бреннер[70], Г. Вайман[71], Д. Деннинг[72], М. Кавелти[73], Э. Каплан[74], Дж. Карр[75], Д. Кларк[76], Б. Коллин[77], П. Левин[78], Дж. Льюис[79], К. Уилсон[80], М. Штоль[81], У. Швартау[82].

---

[58] Thomas T. Cyber Silhouettes. Shadows Over Information Operations / Timothy L. Thomas. – Foreign Military Studies Office (FMSO). Fort Leavenworth, KS, 2005. – 334 p.; Thomas T. Is the IW Paradigm Outdated? A Discussion of U.S. IW Theory / Timothy L. Thomas // Journal of Information Warfare. – 2/3. – 2003. – P.109-116.

[59] Toffler A. War and Anti-War: Survival at the Down of the Twenty-First Century / Alvin and Heidi Toffler. – 1st ed. – 1993. – 302 p.

[60] Wilson, Clay. Information Operations, Electronic Warfare and Cyberwar: Capabilities and Related Policy Issues [Электронный ресурс] // Congress Research Service Report. March 20, 2007. – URL: http://www.fas.org/sgp/crs/natsec/RL31787.pdf (дата обращения: 05.04.14).

[61] Winterfeld S. The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice / Steve Winterfeld, Jason Andress. – Syngress, 2012. – 164 p.

[62] Schwartau W. Information Warfare: Chaos on the Electronic Superhighway / Winn Schwartau. – N.Y.: Thunders Month Press, 1994. – 432 p.

[63] Голубев В.А. «Кибертерроризм» – миф или реальность [Электронный ресурс] // Центр исследования компьютерной преступности. – URL: http://www.crime-research.ru/library/terror3.htm (дата обращения: 05.04.14).

[64] Касперский Е. Компьютерное зловредство / Е. Касперский. – Спб: Питер, 2008. – 208 с.

[65] Лопатин В.Н. Информационная безопасность России: Человек, общество, государство / В.Н. Лопатин. – М.: 2000. – 428 с.

[66] Смолян Г.Л. Сетевые информационные технологии и проблемы безопасности личности / Г.Л. Смолян // Информационное общество. – 1999. – № 1. – С. 21-25.

[67] Стрельцов А.А. Обеспечение информационной безопасности России / А.А. Стрельцов. – М.:МЦНМО, 2002. – 296 с.

[68] Федоров А.В. Супер терроризм: новый вызов нового века / под ред. А.В. Федорова. – М.: Права человека, 2002. – 392 с.

[69] Aldrich, Richard W. Cyberterrorism and Computer Crimes: Issues Surrounding the Establishment of an International Legal Regime [Электронный ресурс] // INSS Occasional Paper 32. Information Operations Series. April 2000. – URL: http://www.au.af.mil/au/aul/bibs/infowar/if.htm (дата обращения: 05.04.14).

[70] Brenner J. America the Vulnerable / Joel Brenner. – New York: Penguin Press, 2011. – 308 p.

[71] Weiman G. Terror on the Internet: the New Arena, the New Challenges / Gabriel Weimann. – Washington, D.C.: United States Institute of Peace Press. – 2006. – 309 p.

[72] Denning D. Reflections on Cyberweapons Controls / Dorothy E. Denning // Computer Security Journal. – Fall 2000. – Vol. XVI. – No. 4. – P. 43-53; Denning, Dorothy. Cyberterrorism [Электронный ресурс] / George Town University. May 23, 2000. – URL: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html; Denning, Dorothy. Is cyberterror next? [Электронный ресурс] / Social Science Research Counsil. November 1, 2001. – URL: http://essays.ssrc.org/sept11/essays/denning.htm (дата обращения: 05.04.14).

[73] Cavelty M. Cyber-security and threat politics: US efforts to secure the information age / Myriam Dunn Cavelty. – New York : Routledge, 2007. – 182 p.

[74] Kaplan, Eben. Terrorists and the Internet [Электронный ресурс] / Counsil on Foreign Relations. January 8, 2009. – URL: http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005 (дата обращения: 05.04.14).

[75] Carr J. Inside Cyber Warfare / Jeffrey Carr. – O'REILLY, 2010. – 213 p.

[76] Clarke, David and Landau, Susan. Untangling Attribution [Электронный ресурс] / National Academy Press. July 15, 2010. – URL: http://www.nap.edu/openbook.php?record_id=12997&page=25 (дата обращения: 05.04.14).

[77] Collin, Barry. The Future of Cyberterrorism [Электронный русурс] // Crime and Justice International. March 1997. – Vol. 13 – Issue 2. – URL: http://www.cjimagazine.com/archives/cji4c18.html?id=415 (дата обращения: 05.04.14).

Вопросы обеспечения информационной безопасности охватывают правовые аспекты, связанные, в частности, с использованием государствами киберпространства в военно-политических целях. Здесь заслуживают внимания работы таких зарубежных исследователей, как Р. Алдрих[83], Д. Грэхам[84], Дж. Данлап[85], К. Дам, Р. Кларк[86], Х. Лин[87], В. Оувенз, М. Роскини[88], Т. Уингфилд[89], С. Уотс[90], С. Шелберг[91], М. Шмитт[92],

[78] Levin P. Securing the Information Highway: How to Enhance the United States Electronic Defenses / Peter L. Levin and Wesley K. Clark // Foreign Affairs. – November/December 2009. – Vol. 88. No. 6. – P. 5-17.
[79] Lewis, James. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats [Электронный ресурс] / Center for Strategic and International Studies. December 2002. – URL: http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf; Lewis, James. Thresholds for Cyberwar [Электронный ресурс] / Center for Strategic and International Studies. September 2010. – URL: http://csis.org/files/publication/101001_ieee_insert.pdf (дата обращения: 05.04.14).
[80] Wilson, Clay. Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress [Электронный ресурс] / Congress Research Center Report. October 17, 2003. – URL: http://fpc.state.gov/documents/organization/26009.pdf; Wilson, Clay. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress [Электронный ресурс] / Congress Research Service Report. January 28, 2008. – URL: http://fpc.state.gov/documents/organization/102643.pdf (дата обращения: 05.04.14).
[81] Stohl M. Cyber Terrorism: A Clear and Present Danger, The Sum of All Fears, Breaking Point or Patriot Games?/ Michael Stohl // Crime, Law and Social Change, Vol. 46, #4. – 2006. – P. 223-238.
[82] Schwartau W. Cyber Shock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists, and Weapons of Mass Disruption / Winn Schwartau. – New York: Thunder's Mouth Press, 2000. – 470 p.
[83] Aldrich, Richard W. The International Legal Implications of Information Warfare [Электронный ресурс] // Airpower Journal. – Fall 1996, – Vol. 10. No. 3. – P. 99-110. – URL: http://www.airpower.maxwell.af.mil/airchronicles/apj/apj96/fall96/aldrich.pdf (дата обращения: 05.04.14).
[84] Graham D. Cyber Threats and the Law of War / David E. Graham // Journal of National Security Law. – August 13, 2010. – Vol. 4 (1). – P. 87-102.
[85] Dunlap C. Jr. Perspectives for Cyber Strategists on Law for Cyberwar / Charles J. Dunlap Jr. // Strategic Studies Quarterly. – Spring 2011. – P. 81-99.
[86] Clarke, Richard A. Securing Cyberspace Through International Norms [Электронный ресурс] / Good Harbor Security Risk Management. – URL: http://www.goodharbor.net/media/pdfs/SecuringCyberspace_web.pdf (дата обращения: 05.04.14).
[87] Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities / Eds. William Owens, Kenneth Dam, and Herbert Lin. – Washington: National Academies Press, 2009. – 367 p.
[88] Roscini M. World Wide Warfare – Jus ad Bellum and the Use of Cyber Force / A. von Bogdandy and R. Wofrum (eds.) // Max Planck Yearbook of United Nations Law. – 2010. – Vol. 14. – P. 85-130.
[89] Wingfield T.C. Legal Aspects of Offensive Information Operations in Space / Thomas L. Wingfried // Journal of Legal Studies. – 1998/1999. – Vol. 9. – P. 121-146.
[90] Watts, Susan. Proposal for cyber war rules of engagement [Электронный ресурс] / BBC News. February 3, 2011. – URL: http://news.bbc.co.uk/2/hi/programmes/newsnight/9386445.stm (дата обращения: 05.04.14).
[91] Schjolberg, Stein and Ghernaouti-Helie, Solange. A Global Treaty on Cybersecurity and Cybercrime [Электронный ресурс] – Second edition. 2011. – 89 p. – URL: http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf (дата обращения: 05.04.14).
[92] Schmitt M. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework / Michael N. Schmitt // Columbia Journal of Transnational Law. – 1999. – Vol. 37. – No. 3. – P. 885-938; Schmitt M. The Principle of Discrimination in 21st Century Warfare / Michael N. Schmitt // Yale Human Rights and Development Law Journal. – 1999. – Vol. 2. – P. 143-182; Schmitt, Michael N. Wired warfare: Computer network attack and jus in bello [Электронный ресурс] // IRRC. June 2002. – Vol. 84. No 846. – P. 365-399. – URL: http://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf (дата обращения: 05.04.14).

Д. Эллиотт[93]; а также российских экспертов в области МИБ таких, как С.М. Бойко, И.Н. Дылевский, С.А. Комов, С.В. Коротков, А.Н. Петрунин, Т.А. Полякова[94], А.А. Стрельцов[95].

Механизмы обеспечения информационной безопасности требуют сбалансированных политико-правовых решений по вопросам, связанным с обеспечением прав и свобод человека и гражданина, включая право на самовыражение и свободу слова, неприкосновенность частной жизни, защиту прав интеллектуальной собственности и другие, поиск которых в своих работах ведут российские авторы: С.А. Бабкин[96], В.Б. Наумов[97], Ю.А. Родичев[98] и др., а также зарубежные исследователи – Дж. Гарсон[99], М. Джаспер[100], С. Курие[101], Л. Лессиг[102], Р. Маккинон[103], Э. Мюррей[104], Р. Олван[105], Р. Спинелло[106], Дж. Хиллер[107], Э. Чадвик[108], Б. Шнайер[109].

---

[93] Elliott, David. Weighing the Case for a Convention to Limit Cyberwarfare [Электронный ресурс] / Arms Control Association. November 2009. – URL: http://www.armscontrol.org/act/2009_11/Elliott (дата обращения: 05.04.14).

[94] Международная информационная безопасность: проблемы и решения / Под общей ред. Комова С.А. – М., 2011. – 264 с.

[95] Стрельцов А.А. Направления совершенствования правового обеспечения информационной безопасности Российской Федерации / А.А. Стрельцов // Информационное общество. – 1999. – № 6. – С. 15-20.

[96] Бабкин С.А. Интеллектуальная собственность в Интернет / С.А. Бабкин. – М.: АО «Центр ЮрИнфоР», 2006. – 512 с.

[97] Наумов В.Б. Право и Интернет: очерки теории и практики / В.Б. Наумов. – М.: Книжный дом «Университет», 2002. – 430 с.

[98] Родичев Ю.А. Информационная безопасность: Нормативно-правовые аспекты: Учебное пособие. – СПб.: Питер, 2008. – 272 с.

[99] Garson D. Computer Technology and Social Issues / David G. Garson. – Harrisburg, Pa.: Idea Group, 1995. – 444 p.

[100] Jasper M. Privacy and the Internet: Your Expectations and Rights Under the Law / Margaret C. Jasper. – NY: Oceana Publications, 2003. – 218 p.

[101] Currie S. Online privacy / Stephen Currie. – San Diego, CA: ReferencePoint Press, 2012. – 96 p.

[102] Lessig L. Code and Other Laws of Cyberspace / Lawrence Lessig. – New York: Basic Books, 1999. – 297 p.

[103] MacKinnon R. Consent of the Networked: the World-Wide Struggle for Internet Freedom / Rebecca MacKinnon. – New York: Basic Books, 2013. – 314 p.

[104] Murray A. Information Technology Law: The Law and Society / Andrew Murray. – Oxford, United Kingdom: Oxford University Press, 2013. – 602 p.

[105] Intellectual Property and Development: Theory and Practice / ed. by Rami M. Olwan. – New York : Springer, 2013. – 392 p.

[106] Spinello R. Cyber Ethics: Morality and Law in Cyberspace / Richard A. Spinello. – Boston: Jones and Bartlett Publishers, 2003. – 238 p.;

[107] Hiller J. Internet Law & Policy / Janine S. Hiller, Ronnie Cohen. – N.J.: Prentice Hall, 2002. – 377 p.

[108] Chadwick A. Internet Politics: States, Citizens, and New Communication Technologies / Andrew Chadwick. – New York: Oxford University Press, 2006. – 384 p.

[109] Schneier, Bruce. The Eternal Value of Privacy [Электронный ресурс] // Wired Magazine. May 18, 2006. - URL: http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886 (дата обращения: 06.04. 14).

Вопросы управления Интернетом приобрели особую актуальность в контексте информационной безопасности. В этой связи были изучены работы следующих российских и зарубежных исследователей: Э. Гелбстайна[110], Дж. Голдсмита[111], Е.С. Зиновьевой[112], Р. Кнейка[113], К. Кукьера[114], Й. Курбалия, Д. Лонга[115], Дж. Малколма[116], Р. Мансела[117], Дж. Матиасона[118], М. Мюлера[119], Д.Н. Пескова[120], В. Серфа[121].

Отдельное внимание в данном исследовании уделено вопросам обеспечения МИБ, научно-исследовательскую основу по которым составляют работы следующих российских авторов и экспертов в области информационной безопасности: И.Ю. Алексеевой[122], А.В. Бедрицкого, Д.С. Вотрина, С.Н. Гриняева[123], А. Зуева[124], А.В. Крутских, И.Н. Панарина и

[110] Kurbalija J. Internet Governance: Issues, Actors and Divides/ Jovan Kurbalija and Eduardo Gelbstein. – Diplo Foundation and the Global Knowledge Partnership, 2005. – 144 p.
[111] Goldsmith J. Who controls the Internet?: Illusions of a Borderless World / Jack Goldsmith and Tim Wu. – New York: Oxford University Press, 2006. – 226 p.
[112] Зиновьева Е.С. Международное управление Интернетом: конфликт и сотрудничество: Учебное пособие / Е.С. Зиновьева. – МГИМО-Университет, 2011. – 169 с.
[113] Knake R. Internet Governance in the Age of Cyber Insecurity / Robert K. Knake. – New York: Council on Foreign Relations, 2010. – 43 p.
[114] Cukier, Kenneth Neil. Who Will Control Internet? [Электронный ресурс] // Foreign Affairs. – November/December 2005. – URL: http://www.foreignaffairs.com/articles/61192/kenneth-neil-cukier/who-will-control-the-internet (дата обращения 05.04.14).
[115] Long D. Protect your privacy: How to Protect Your Identity As Well As Your Financial, Personal, and Computer Records in An Age of Constant Surveillance / Duncan Long. – Guilford, Conn.: Lyons Press, 2007. – 277 p.
[116] Malcolm J. Multi-stakeholder Governance and the Internet Governance Forum / Jeremy Malcolm. – Perth: Terminus Press, 2008. – 611 p.
[117] Mansell R. Imagining the Internet: Communication, Innovation, and Governance / Robin Mansell. – Oxford: Oxford University Press, 2012. – 289 p.
[118] Mathiason J. Internet Governance: the New Frontier of Global Institutions / John Mathiason. – New York: Routledge, 2009. – 178 p.
[119] Mueller M.L. Networks and States: the Global Politics of Internet Governance / Milton L. Mueller. – Cambridge, Mass: MIT Press, 2010. – 313 p.
[120] Песков Д.Н. Интернет в мировой политике: формы и вызовы // Современные международные отношения и мировая политика / отв. ред. А.В. Торкунов. – М.: «Просвещение», 2004. – С.222-246.
[121] Cerf V. On the Evolutions of Internet Technologies / Vint Cerf // Proceedings of the IEEE. – Vol.92. – Issue 9, 2004 – P. 1360-70; Cerf, Vint. Looking Toward the Future [Электронный ресурс] // The Internet Protocol Journal – Vol.10, No. 4. – URL: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_future.html (дата обращения: 05.04.14).
[122] Информационные вызовы национальной и международной безопасности / И.Ю. Алексеева и др. Под общей редакцией А.В. Федорова, В.Н. Цигичко. – М.: ПИР-Центр, 2001. – 328 с.;
[123] Гриняев С.Н. Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. – Мн.: Харвест, 2004. – 448 с.
[124] Зуев А. Безопасность в виртуальном пространстве // Мировая экономика и международные отношения. – 2003. – № 9. – С. 13-17.

Л.Г. Панариной[125], И.Л. Сафроновой, А.И. Смирнова[126], Г.Л. Смоляна, А.А. Стрельцова[127], А.М. Тарасова[128], А.В. Федорова[129], В.Н. Цыгичко, Д.С. Черешкина[130], В.П. Шерстюка[131].

В числе российских авторов, которые занимаются исследованием различных аспектов киберполитики США, основными являются А.В. Бедрицкий[132], В. Жуков[133], С.А. Комов[134], С.В. Коротков, Г.Б. Корсаков[135], А.А. Леваков[136], В. Пашков[137], С.М. Рогов[138], Е.А. Роговский[139], П.А. Шариков[140]. Главное отличие данного исследования

---

[125] Панарин И.Н. Информационная война и мир / И.Н. Панарин, Л.Г. Панарина. – М.: ОЛМА-ПРЕСС, 2003. – 384 с.; Панарин И.Н. Информационная война и власть. / И.Н. Панарин. – М., 2001. – 224 с.

[126] Глобальная безопасность в цифровую эпоху: стратагемы для России. Под общ. ред. Смирнова А.И. – М.: ВНИИгеосистем, 2014. – 394 с.

[127] Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В.А. Садовничего и В.П. Шерстюка. – М., МЦНМО, 2002. – 296 с.

[128] Тарасов А.М. Электронное правительство и информационная безопасность: учебное пособие // СПб.: ГАЛАРТ. – 2011. – 648 с.

[129] Федоров А.В. Информационная безопасность в мировом политическом процессе: учеб. пособие. / А.В. Федоров. – М.: МГИМО-Университет, 2006. – 220 с.; Федоров А.В. Особенности современной информационной борьбы и международное сотрудничество в области информационной безопасности / А.В. Федоров // Информационная безопасность / Под ред. В.Г. Матюхина и др. – М.: МГФ «Знание» ГЭИТИ, 2005. – С. 464-481.

[130] Информационное оружие – новый вызов международной безопасности / Цыгичко В.Н., Вотрин Д.С., Крутских А.В., Смолян Г.Л., Черешкин Д.С. – М.: Институт системного анализа РАН, 2000. – 52 с.; Черешкин Д.С. Проблемы управления информационной безопасностью / Д.С. Черешкин. – М.: Едиториал УРСС, 2002. – 224 с.

[131] Шерстюк В.П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральные и региональные аспекты обеспечения национальной безопасности / В.П. Шерстюк // Информационное общество – 1999. – №5. – С. 3-5.

[132] Бедрицкий А.В. Эволюция американской концепции информационной войны / А.В. Бедрицкий // М.: РИСИ. Аналитические обзоры. Выпуск №3, 2003. – 26 с.; Бедрицкий А.В. Информационная война: концепции и их реализация в США / А.В. Бедрицкий // М.: РИСИ, 2008. – 183 с.; Бедрицкий А.В. Американская политика контроля над кибернетическим пространством / А.В. Бедрицкий // Проблемы национальной стратегии. – 2010. – №2 (3). – С. 25-40.

[133] Жуков В. Взгляды военного руководства США на ведение информационной войны / В. Жуков // Зарубежное военное обозрение. – 2001. – №1. – С. 2-8.

[134] Международная информационная безопасность: дипломатия мира. Сборник статей / под общ. редакцией С.А.Комова. – М., 2009. – 272 с.

[135] Корсаков Г. Информационное оружие супердержавы / Г. Корсаков // Пути к миру и безопасности. – М.: ИМЭМО РАН, 2012. – Выпуск 1 (42). – С. 34-60.

[136] Леваков А.А. Анатомия информационной безопасности США [Электронный ресурс] // Jet Info. – 2002. – №12 (115) – URL: http://www.jetinfo.ru/Sites/new/Uploads/2002_6.DF9C812FFBD9496BAE9694E27F2D9D1D.pdf; Леваков А.А. Новые приоритеты в информационной безопасности США [Электронный ресурс]. – URL: http://www.agentura.ru/equipment/psih/info/prioritet/ (дата обращения: 05.04.14).

[137] Пашков В. Информационная безопасность США / В. Пашков // Зарубежное военное обозрение. – 2010. – №10. – С. 3-13.

[138] Рогов С.М. Стратегия национальной безопасности администрации Обамы, американское лидерство в многополярном мире [Электронный ресурс] // Независимое военное обозрение. 11 июня 2010. – URL: http://nvo.ng.ru/authors/4176/?PAGEN_1=2 (дата обращения: 05.04.14).

[139] Роговский Е.А. Кибербезопасность и кибертерроризм / Е.А. Роговский // США, Канада: Экономика, политика, культура. – 2003. – №8. – С. 23-41.; Роговский Е.А. США: информационное общество / Е.А. Роговский. – М.: Международные отношения, 2008. – 408 с.; Роговский Е.А. Американская стратегия

заключается в комплексном рассмотрении политики США по вопросам обеспечения информационной безопасности на национальном и международном уровнях с учетом действующей американской концепции угроз в данной сфере.

Источниковую базу исследования составляют следующие группы документов:

1. Нормативно-правовые документы Соединенных Штатов Америки: указы и директивы президента США, федеральные законодательные акты, национальные стратегии, затрагивающие вопросы обеспечения информационной безопасности страны, а также военные доктрины и стратегии по ведению операций в киберпространстве.

2. Пресс-релизы Белого Дома, министерств и ведомств США, выступления, комментарии и интервью официальных лиц США.

3. Аналитические обзоры, доклады и отчеты министерств и относящихся к ним комиссий, корпорации РАНД (RAND), Центра стратегических и международных исследований (CSIS), Главного контрольно-финансового управления США (GAO), исследовательской службы Конгресса США (CRS).

4. Официальные документы (резолюции, конвенции, стратегии, руководящие принципы, доклады рабочих и экспертных групп) таких международных организаций, как «Большая восьмерка», Организация экономического сотрудничества и развития, Совет Европы, Организация Объединенных Наций, Организация по безопасности и сотрудничеству в Европе, Организация Североатлантического договора, Международный

информационного преобладания // Россия и Америка в XXI веке. Электронный журнал. – 2009. – №3. – URL: http://www.rusus.ru/?act=read&id=161%9A; Роговский Е.А. Глобальные информационные технологии – фактор международной безопасности / Е.А. Роговский // США, Канада: Экономика, политика, культура. – 2010. – №12. – С.3-26.; Роговский Е.А. Политика США по обеспечению безопасности киберпространства / Е.А. Роговский // США, Канада: Экономика, политика, культура. – 2012. – №6. – С. 3-22.

[140] Шариков П.А. Политика США в области информационной безопасности: автореф. дис. канд. полит. наук: 23.00.04 / Институт США и Канады РАН. – М., 2009. – 34 с.; Шариков П.А. Развитие информационных ресурсов как фактор американского могущества в современном мире // Россия и Америка в XXI веке. Электронный журнал. – 2009. – №2. – URL: http://www.rusus.ru/?act=read&id=153; Шариков П.А. Китайские киберугрозы национальной безопасности США / П.А. Шариков // США, Канада: Экономика, политика, культура. – 2013. №11. – С. 21-37.

союз электросвязи, Организация американских государств, Шанхайская организация сотрудничества и Форум «Азиатско-Тихоокеанского экономического сотрудничества»; итоговые документы двух этапов Всемирной встречи на высшем уровне по вопросам информационного общества; двусторонние соглашения и договоренности по вопросам обеспечения информационной безопасности.

5. Статистические и аналитические материалы организаций, занимающихся вопросами информационной безопасности: Симантек (Symantec), Касперский (Kaspersky), Мандиант (Mandiant), МакАфи McAfee), Нортон (Norton), Джавелин Стратеджи и Ресерч (Javelin Strategy and Research).

Объектом исследования в диссертации является информационная безопасность США.

Предмет исследования – концепция угроз информационной безопасности США и ее международно-политическая составляющая.

Хронологические рамки исследования полностью охватывают период активного формирования стратегии информационной безопасности США (с начала 1990-х годов по настоящее время), что соответствует периодам президентства Билла Клинтона, Джорджа Буша-мл. и Барака Обамы.

Цели и задачи исследования. Диссертация преследует следующую основную цель – анализ подходов США к обеспечению информационной безопасности на национальном и международном уровнях.

Достижению данной цели служит решение следующих задач:

- выявить и рассмотреть основные угрозы информационной безопасности США;
- определить основные элементы национальной стратегии США в киберпространстве;
- проанализировать нормативно-правовые основы деятельности США в области обеспечения информационной безопасности;

- исследовать международно-политическую составляющую американской концепции обеспечения информационной безопасности;
- сформулировать потенциальные направления дальнейшего сотрудничества Российской Федерации и Соединенных Штатов в рамках международного диалога по вопросам обеспечения МИБ.

Теоретическая и методологическая основа исследования. Изучение информационной безопасности является формирующимся самостоятельным научно-исследовательским направлением, лежащим в плоскости междисциплинарного знания. В центре внимания данного исследования находится государство как ключевой актор международных отношений, а раскрытие темы происходит через такие понятия, как угрозы национальной безопасности, национальные интересы, государственное противоборство в информационной сфере и другие, присущие в целом реалистической традиции. При этом автор придерживается принципов неореализма и исходит из того, что США определяют внешнюю политику в исследуемой области на основании национальных интересов и стремления обеспечить лидерство в международной системе. В то же время сама специфика сферы ИКТ гораздо шире и может рассматриваться с точки зрения других теоретических парадигм международных отношений. Также в рамках данного исследования были приняты во внимание теоретические подходы к информационной войне Дж. Аркуиллы, Д. Деннинг, М. Либики, Д. Ронфельда, Т. Томаса, К. Уилсона, С. Уинтерфельда и В. Швартау.

Методологическую основу диссертационного исследования составляют методы современного научного познания, используемые в политической науке. Системный подход позволил представить киберполитику США в ее целостном виде, состоящей из взаимосвязанных элементов внутренней и внешней политики. В свою очередь сравнительный метод был использован в целях выявления различий и точек

соприкосновения в позициях стран по вопросам МИБ. Также использован описательный метод, посредством которого было раскрыто содержание угроз в области информационной безопасности и даны их ключевые характеристики. Историко-описательный метод позволил рассмотреть эволюцию подходов США к обеспечению информационной безопасности и развитие международного диалога по вопросам МИБ. С использованием метода анализа документов была изучена нормативно-правовая база США, а также основополагающие документы международных организаций по вопросам обеспечения информационной безопасности (всего более ста документов), выявлены основные составляющие национальной стратегии США в области обеспечения информационной безопасности, а также актуальные политико-правовые тенденции. Метод кейсов (case study) был применен для проведения анализа конкретных примеров деструктивного использования ИКТ, выявления их характеристик и последствий для национальной и международной безопасности.

Научная новизна данной работы заключается в следующем:

- Выявлена действующая концепция угроз информационной безопасности США, включающая в себя угрозы военно-политического, криминального и террористического характера. Установлено, что угрозы в информационном пространстве носят универсальный и глобальный характер.
- Проанализирована и систематизирована широкая база основополагающих официальных документов США и международных организаций в области обеспечения информационной безопасности, многие из которых рассмотрены впервые в российских исследованиях.
- Проведено комплексное исследование подходов США к обеспечению информационной безопасности, охватывающее как национальный, так и внешнеполитический уровень. Выявлены основные тенденции политики США, ключевые приоритеты и составляющие стратегии действий США в киберпространстве.

- Сформулированы потенциальные направления дальнейшего сотрудничества Российской Федерации с Соединенными Штатами по вопросам обеспечения МИБ на двустороннем и многостороннем уровне.

Теоретическая и практическая значимость исследования заключается в возможности его использования в политико-аналитической, научной и преподавательской деятельности.

Проведенный комплексный анализ политики США в области обеспечения информационной безопасности в контексте актуальных вопросов международной информационной безопасности дает представление не только о стратегии США в данной сфере, но и демонстрируют расстановку политических сил в глобальном информационном пространстве.

Выявленные механизмы обеспечения информационной безопасности, а также предложенный обзор нормативно-правовой базы США могут быть учтены при разработке российских национальных и военных стратегий, доктрин, законодательных актов в области информационной безопасности как в целях применения наилучших практик, так и с целью сбалансировать политику США как одного из главных игроков в глобальном информационном пространстве. Результаты исследования могут быть использованы при подготовке позиционных материалов и выработке переговорной линии с Соединенными Штатами и их союзниками по вопросам обеспечения информационной безопасности.

Кроме того, материалы исследования могут быть использованы в рамках учебного процесса в качестве составляющей курсов и пособий по вопросам международной информационной безопасности, роли ИКТ в современных международных отношениях, а также по вопросам национальной и международной безопасности.

Положения, выносимые на защиту:

1. Проведенный анализ позволил установить, что при осуществлении мер по обеспечению информационной безопасности на национальном

уровне США учитывают комплекс информационных угроз военно-политического, преступного и террористического характера. Данная концепция в целом соответствует видению большинства стран, участвующих в международном диалоге по вопросам обеспечения информационной безопасности. При этом важным сохраняющимся различием в подходах стран является определение границ информационной безопасности.

2. Обеспечение информационной безопасности требует комплексного подхода не только на национальном, но и на внешнеполитическом уровне. В этой связи продвигаемая Соединенными Штатами в период администраций Б. Клинтона и Дж. Буша-мл. международная концепция обеспечения информационной безопасности, исключающая военно-политическое измерение, доказала свою неэффективность. В результате администрация Б. Обамы в существенной степени усилила международный вектор национальной стратегии кибербезопасности и поставила задачу по достижению лидерства в многостороннем процессе обеспечения информационной безопасности в целях создания необходимых условий для продвижения американских инициатив в данной сфере.

3. Как показал опыт США, усиление мер противодействия угрозам информационной безопасности и в целом национальной безопасности связано с повышением уровня государственного контроля за киберпространством и деятельностью пользователей в Сети. В этих условиях США вынуждены искать приемлемый баланс между обеспечением безопасности и соблюдением прав и свобод граждан. Несмотря на риторику руководства страны о важности соблюдения прав и свобод в информационном пространстве, данная дилемма решается в США в пользу обеспечения безопасности.

4. При обеспечении информационной безопасности США делают ставку на механизмы киберсдерживания, оставляя за собой право использовать любые необходимые средства, включая военные, в ответ на

враждебные действия в киберпространстве. При этом США исходят из необходимости снижения риска проведения деструктивных кибератак, в том числе упреждающими действиями, которые, в свою очередь, предусматривают ведение широкого спектра информационных операций.

5. Основными формами межгосударственного противоборства в информационном пространстве становятся информационные войны и кибершпионаж. Наращивание странами киберпотенциала ведет к милитаризации киберпространства, что может стать существенным фактором, подрывающим международную стабильность и безопасность. При этом на международном уровне возникает правовой вакуум в связи с отсутствием общепринятых международных норм, регулирующих враждебное использование ИКТ государствами, а также правил поведения государств в киберпространстве. Ликвидация этого вакуума требует разработки эффективных международных механизмов и специальной международной политико-правовой базы в данной сфере.

6. Важным условием для США является сохранение свободы действий в киберпространстве. Данной задаче служат внешнеполитические инициативы США, направленные на сохранение механизмов управления Интернетом, а также на ограничение развития международной политико-правовой базы, регулирующей деятельность государств в информационном пространстве, рамками необязывающих политических документов.

7. С учетом сохраняющихся различий в подходах к международным механизмам обеспечения информационной безопасности таких ключевых игроков, как Россия и США, дальнейшее развитие политико-правовых механизмов регулирования сферы МИБ возможно в первую очередь в рамках направлений, представляющих общий интерес. Такими направлениями на сегодняшний день являются: выработка общих подходов к угрозам информационной безопасности и мерам по их устранению в рамках Группы правительственных экспертов ООН по МИБ, разработка общепринятых правил поведения государств в киберпространстве, а также

формирование перечня мер по укреплению доверия в киберпространстве. Поступательная проработка вопросов МИБ в рамках двусторонних и многосторонних практических договоренностей также будет способствовать повышению уровня доверия между государствами и формировать основу будущего универсального режима МИБ.

Апробация основных положений диссертационного исследования была проведена на заседании кафедры мировых политических процессов МГИМО (У) МИД России. Материалы исследования были использованы при проведении курса «Международная информационная безопасность» для студентов, обучающихся по магистерской программе Европейского учебного института при МГИМО (У) МИД России, а также в ходе круглого стола «Информационная безопасность государства в современных международных отношениях» (МГИМО (У) МИД России, 20 июня 2014 г.).

II. СТРУКТУРА И СОДЕРЖАНИЕ РАБОТЫ

Структура работы определена ее целью и задачами. Диссертационное исследование состоит из введения, трех глав, заключения, списка сокращений, а также списка использованных источников и литературы.

Во введении обосновывается актуальность диссертационной работы, определяется объект, предмет, цель и задачи исследования, раскрывается научная новизна, оценивается степень разработанности проблемы, характеризуется теоретико-методологическая основа исследования, отмечается теоретическая и практическая значимость работы, сформулированы положения, выносимые на защиту, а также представляется апробация ее основных положений и выводов.

В первой главе «Концепция угроз информационной безопасности США» выявляются основные угрозы информационной безопасности США и рассматривается их содержание.

В параграфе 1.1 «Классификация угроз информационной безопасности» рассматриваются подходы американских консультативных органов, а также министерств и ведомств к существующим угрозам в информационной сфере. Проведенное в данной части исследование позволило сформулировать общую концепцию угроз информационной безопасности США, которая включает в себя угрозы военно-политического, преступного и террористического характера, а также соотнести основных акторов с видами угроз, указать возможные мотивы злонамеренного использования ИКТ и наиболее привлекательные объекты для проведения кибератак.

Источниками угроз в киберпространстве являются многочисленные акторы. Однако основная угроза по-прежнему исходит от государств и действующих в их интересах посредников, которые обладают необходимыми навыками и технологиями для проведения наиболее деструктивных действий в киберпространстве. Киберугрозы требуют разработки комплекса мер по противодействию, охватывающего три основных уровня обеспечения безопасности – государство, частные компании и организации, индивидуальные пользователи.

В параграфе 1.2 «Информационные войны» раскрывается содержание угрозы использования ИКТ государствами в военно-политических целях.

На международном уровне формируется тенденция к использованию государствами ИКТ в качестве кибероружия не только в ходе военных операций, но и для обеспечения военно-политических целей без перехода к стадии открытой военной конфронтации. С точки зрения национальной безопасности основную озабоченность США вызывают возрастающий киберпотенциал и действия других государств, направленные на подрыв американской военной информационной инфраструктуры, критической инфраструктуры страны и систем жизнедеятельности общества и государства.

Кибератаки могут стать причиной эскалации межгосударственного конфликта как в кибер-, так и в физическом пространстве, так как, с одной стороны, в условиях глобального развития сетевых технологий сложно рассчитать и предусмотреть их масштаб и последствия, с другой – ответные меры пострадавшей стороны могут быть непропорциональными в связи со сложностью установления источника и вероятностью ошибочной оценки ситуации. В этой связи возрастает потребность в международных механизмах регулирования поведения государств в информационной сфере.

В параграфе 1.3 «Кибершпионаж» отмечается, что с развитием ИКТ методы кибершпионажа стали доступны как государствам, традиционно осуществляющим разведывательную деятельность, так и негосударственным акторам.

Наибольшую угрозу национальной безопасности США представляет экономический шпионаж, проводимый государствами или их посредниками, целью которого является получение чувствительной информации и коммерческих секретов в стратегически важных областях. Кроме того, США столкнулись с возрастающей угрозой со стороны отдельных индивидов, использующих авторизированный доступ к информации в идеологических целях. Разоблачения «Викиликс» и Э. Сноудена имели целый ряд политических последствий для США, став причиной пересмотра принципов деятельности разведывательных служб США, а также американской политики по комплексу вопросов обеспечения информационной безопасности и управлению Интернетом.

В параграфе 1.4 «Киберпреступность» рассматриваются основные группы и виды киберпреступлений. Отмечается устойчивый рост числа киберпреступлений, а также наносимый ими ущерб отдельным пользователям, предприятиям и в целом экономике США, что имеет свои последствия для национальной безопасности и экономической стабильности.

Особенность киберпреступлений заключается в том, что они чаще носят трансграничный характер и требуют проведения транснациональных расследований и сбора доказательной базы. То есть национальные усилия должны подкрепляться эффективными механизмами межгосударственного взаимодействия, что, в свою очередь, требует наличия соответствующей международной политико-правовой базы.

В параграфе 1.5 «Кибертерроризм» рассматривается новая форма терроризма – кибертерроризм. После событий 11 сентября 2001 года терроризм в США был отнесен к одной из главных угроз национальной безопасности. Развитие ИКТ существенно расширяет возможности террористических групп, которые в настоящее время активно используют новые технологии в ежедневной операционной деятельности и в целом аналогично вооруженным силам прибегают к методам информационных операций. Несмотря на то, что угроза проведения кибертеррактов в чистом виде, то есть исключительно посредством применения ИКТ, остается во многом гипотетической, специалисты США озабочены использованием ИКТ в качестве «усилителя» традиционных методов террористической деятельности и уделяют существенное внимание деятельности террористических групп в информационном пространстве.

Вторая глава «Нормативно-правовые основы деятельности США в области обеспечения информационной безопасности» посвящена рассмотрению подходов США к обеспечению информационной безопасности на национальном уровне. Широкий анализ документов США позволил выявить основы национальной стратегии действий в киберпространстве, а также тенденции совершенствования национальной системы обеспечения информационной безопасности.

В параграфе 2.1 «Национальная стратегия кибербезопасности США» рассматриваются президентские директивы и национальные стратегии, формирующие стратегические ориентиры обеспечения кибербезопасности.

Начиная с 2003 года США ведут работу над комплексной стратегией обеспечения безопасности в киберпространстве. При этом если усилия администрации Дж. Буша-мл. были сконцентрированы преимущественно на разработке и развитии национальных программ и систем реагирования на угрозы информационной безопасности, то администрация Б. Обамы существенно развила направление внешнеполитического сотрудничества, что связано с признанием Соединенными Штатами неэффективности односторонних мер обеспечения безопасности в киберпространстве. Таким образом, действующая национальная киберстратегия США включает в себя комплекс мероприятий по защите критической инфраструктуры страны и укреплению национального сегмента информационных сетей и систем, а также полноценную стратегию действий на международной арене по вопросам информационной безопасности.

В параграфе 2.2 «Военная киберстратегия США» проводится анализ положений военной киберстратегии США.

Основной целью вооруженных сил США в киберпространстве является достижение и удержание информационного превосходства. Военные операции с использованием информационного потенциала являются неотъемлемой составляющей военной доктрины США, которые рассматривают киберпространство как полноценную сферу оперативной деятельности наряду с космосом, небом, сушей и морем. Деятельность вооруженных сил США в киберпространстве не ограничивается оборонительными и сдерживающими действиями, а предусматривает широкое использование ИКТ и специально разработанного кибероружия в наступательных целях, что может представлять угрозу национальной безопасности других государств и международной безопасности и стабильности в целом.

В параграфе 2.3 «Федеральные законодательные акты США в области обеспечения информационной безопасности» проводится анализ законодательной базы США по таким направлениям, как защита

критической инфраструктуры страны, повышение уровня защищенности федеральных информационных сетей и систем, а также защита личных данных граждан.

Учитывая быстрый рост числа угроз в области информационной безопасности, информационная инфраструктура США оказалась крайне уязвимой, а государственные и частные структуры не готовы к обеспечению должного уровня безопасности. Как следствие, начиная с 2001 года в США явно прослеживается тенденция к усилению контроля за киберпространством со стороны государства, результатом которого явились злоупотребления в области гражданских прав и свобод.

Важной задачей для Конгресса США становится выработка сбалансированных законодательных инициатив, направленных на повышение уровня безопасности в информационной сфере при соблюдении интересов государства, бизнеса и граждан.

Третья глава «Международная составляющая политики США в области информационной безопасности» освещает инициативы США по противодействию угрозам информационной безопасности на международной арене.

В параграфе 3.1 «Политика США по вопросам управления Интернетом» рассматриваются основы политики США по вопросам управления Глобальной сетью, их позиция в международном многостороннем диалоге.

Интернет является стратегическим ресурсом, который широко используется США в целях обеспечения национальных интересов в экономической, политической, социальной, военной, информационной и других сферах. Для США принципиально важным является сохранение инструментов управления Глобальной сетью, несмотря на попытки международного сообщества внести изменения в действующую систему управления посредством ее интернационализации.

Автор приходит к заключению, что в ближайшей перспективе переход контроля над управлением Интернетом под эгиду какой-либо межправительственной организации в целях обеспечения многостороннего управления пока не состоится. Учитывая политическую важность вопросов управления Сетью, процесс формирования новой системы управления будет непростым и может существенно затянуться.

В параграфе 3.2 «Приоритетные направления внешней политики по вопросам кибербезопасности в период администраций Б. Клинтона и Дж. Буша-мл.» анализируется продвигаемая США на международной арене концепция информационной безопасности, которая включает в себя вопросы противодействия использованию ИКТ в преступных целях, обеспечения безопасности критической инфраструктуры и глобальной культуры кибербезопасности.

Рассмотрены политико-правовые рамки данной концепции, которые определены Конвенцией Совета Европы о киберпреступности 2001 года и Резолюциями ООН «Борьба с преступным использованием информационных технологий» 2000, 2001 гг. и «Создание глобальной культуры кибербезопасности» (принималась в период с 2002 по 2009 год). Делается вывод, что подход США к обеспечению кибербезопасности, не учитывающий всего комплекса угроз, потерял свою актуальность в свете всевозрастающей угрозы использования ИКТ в военно-политических целях.

Выявлена взаимосвязь между усилиями Соединенных Штатов на национальном уровне и внешнеполитическими инициативами. Отмечается, что одной из задач США на международном уровне является разработка механизмов трансграничного сбора и обмена информацией, что, в свою очередь, дополняет меры США по созданию упрощенных схем сбора информации и данных федеральными службами.

В параграфе 3.3 «Эволюция в подходах США по вопросам обеспечения международной информационной безопасности» представлен анализ позиции США по вопросам МИБ в рамках ООН и ее трансформация.

Первый этап (с 1998 по 2008 г.) – период администраций Б. Клинтона и Дж. Буша-мл., этап сдерживания инициатив Российской Федерации, направленных на развитие вопросов, связанных с использованием ИКТ в военно-политических целях, ограничением использования информационного оружия и разработкой международного политико-правового режима информационной безопасности. Незаинтересованность США объясняется проводимой в тот период работой по развитию концепции информационной войны и национальной стратегии ведения информационных операций.

Второй этап (с 2009 по н.в.) – этап реализации стратегии кибербезопасности Б. Обамы, которая предусматривает активизацию участия США в международном диалоге по МИБ. Именно в рамках Группы правительственных экспертов ООН по МИБ США официально признали наличие угрозы информационной безопасности военного характера и в целом включились в работу по всему комплексу вопросов. Это придало импульс развитию международного диалога не только в рамках ООН, но и таких организаций, как «Большая восьмерка» и ОБСЕ.

В параграфе 3.4 «Укрепление роли США в международном диалоге по информационной безопасности в период администрации Б. Обамы» рассматриваются американские инициативы, направленные на формирование механизмов коллективной кибероборонs, разработку мер по укреплению доверия и правил поведения государств в киберпространстве.

В рамках работы с партнерами по НАТО, «Большой восьмерке», ОБСЕ и ЕС Соединенные Штаты предпринимают попытки возглавить международный процесс разработки и формирования механизмов обеспечения информационной безопасности и таким образом сдержать инициативы российской стороны и ее партнеров по созданию универсального режима международной информационной безопасности.

Кибериниициативы США также служат их геополитическим целям, что подтверждает расширение договоренностей с НАТО и рядом других стран, в

том числе Азиатско-Тихоокеанского региона, о коллективной обороне с учетом кибераспектов. В двустороннем формате важным для США является сотрудничество с Китаем и Россией. Достигнутые между странами договоренности направлены на повышение доверия между государствами и закладывают солидный фундамент для дальнейшего развития практических механизмов взаимодействия по вопросам информационной безопасности. В целом правила игры в такой крайне чувствительной сфере, как киберпространство, во многом будут определяться развитием отношений США с Россией и Китаем.

В параграфе 3.5 «Пути формирования международной политико-правовой базы по вопросам обеспечения информационной безопасности» на основе анализа двух конкурирующих подходов к регулированию сферы МИБ, продвигаемых на международной арене Россией и США, делается вывод о том, что на данном этапе компромиссным вариантом формирования международного режима информационной безопасности является путь поступательной разработки практических договоренностей по направлениям, представляющим общий интерес, в том числе в рамках мер по укреплению доверия в киберпространстве и правил поведения государств.

В **заключении** обобщаются результаты проведенного исследования, делаются основные выводы в соответствии с поставленными в диссертации целями и задачами.

Вопросы обеспечения информационной безопасности требуют комплексного подхода к их рассмотрению, а также формирования институциональных и нормативно-правовых рамок как на национальном, так и на международном уровне. Сегодня даже самые технологически развитые страны такие, как Соединенные Штаты Америки, не способны эффективно противостоять угрозам информационной безопасности в одностороннем порядке. В условиях трансграничности угроз возрастает

роль международного сотрудничества и необходимость в разработке универсального режима международной информационной безопасности.

Основные положения диссертации отражены в научных публикациях автора общим объемом около 3,5 п.л. Все публикации по теме диссертации.

В изданиях перечня Высшей аттестационной комиссии при Министерстве образования и науки Российской Федерации:

1. Батуева Е.В. Политика администрации Барака Обамы в области обеспечения информационной безопасности // Вестник МГИМО-Университета. – 2010. – № 4. – С. 271-276. (0,74 п.л.)

2. Батуева Е.В. Виртуальная реальность: концепция угроз информационной безопасности США и ее международная составляющая // Вестник МГИМО-Университета. – 2014. – № 3. – С. 128-136. (1 п.л.)

3. Батуева Е.В. Информационные войны США: к определению национальной киберстратегии // Международные процессы. – Январь-март; апрель-июнь 2014. – Том 12, №1-2 (36-37). – С. 117-127. (0,9 п.л.)

В прочих изданиях:

4. Батуева Е.В. Позиция США в межгосударственном диалоге по вопросам информационной безопасности // Международная мозайка: сборник научных трудов молодых ученых. Выпуск первый/ под ред. О.Н. Барабанова. – М.: МГИМО-Университет, 2006. – С. 141-154. (0,6 п.л.)

5. Батуева Е.В. Политический диалог по вопросам управления Интернетом // Мировая политика: новые проблемы и направления: сборник научных статей / под ред. М.М. Лебедевой. – М. : МГИМО-Университет, 2009. – С. 15-22. (0,3 п.л.)