Политика администрации Барака Обамы в области обеспечения информационной безопасности

Батуева Е. В.

Статья посвящена подходу США к вопросам обеспечения информационной безопасности как на внутриполитическом, так и на внешнеполитическом уровнях. Автор раскрывает дуализм в политике США в отношении комплекса существующих угроз информационной безопасности таких, как киберпреступность, кибертерроризм, использование информационно-коммуникационных технологий государствами в военно-политических целях. В статье содержится анализ мер, предпринимаемых Администрацией Б. Обамы в целях повышения эффективности обеспечения информационной безопасности, проводятся параллели между политическими курсами администраций Б. Клинтона, Дж. Буша и Б. Обамы в области кибербезопасности.

С конца XX столетия мировое сообщество шагнуло в своем развитии из индустриального в постиндустриальный или «информационный» период, отличительной особенностью которого является повсеместное внедрение и использование информационно-коммуникационных технологий (ИКТ) во всех сферах деятельности государства, общества и человека. Количество, технический уровень и доступность информационных ресурсов теперь определяют уровень развития страны и ее роль в международных отношениях.

Произошедшая трансформация пространства, в рамках которого выстраивается взаимодействие государств, все больше погружает как международные отношения, так и внутреннюю политику государств в виртуальный мир или киберпространство. Появление ИКТ породило новую, на этот раз информационную гонку между государствами, которые, благодаря новым технологиям, получили большой набор инструментов для ведения борьбы за обладание информацией, достижение и удержание информационного превосходства.

Безусловно, информационные технологии играют положительную роль в развитии стран. ИКТ оказывают непосредственное влияние на развитие экономической, социальной, культурной и военно-политической сфер деятельности государства и общества, становясь основополагающим фактором обеспечения стабильности и устойчивого развития. Под влиянием информационно-коммуникационных технологий заметно снизилась значимость таких факторов, как пространство и время. Экономики получили значительный импульс при переходе на производства, основанные на автоматизированных системах и последних достижениях в сфере информатики и электроники. Стал возможен обмен информацией, мнениями, товарами и услугами в режиме реального времени на неограниченные расстояния. Возникло глобальное информационное пространство в качестве инфраструктуры современного постиндустриального общества.

Наряду с позитивными изменениями, новые технологии породили целый ряд негативных последствий для мирового сообщества:

— увеличение «цифрового разрыва» между государствами и поляризация мира из-за неравного

Батуева Елена Владимировна — аспирант Кафедры мировых политических процессов МГИМО(У) МИД РФ
email: ebatueva@gmail.com

доступа стран к информационно-коммуникационным технологиям;

— трансформацию угроз международной и национальной безопасности (возникновение киберпреступности, кибертерроризма, информационных атак, воздействие которых направлено на дестабилизацию систем управления государством, вооруженными силами и экономикой). Сетецентричная парадигма, разработанная в США, которые являются лидером в области информационных технологий, подразумевает высокую степень зависимости национальной безопасности от информационной безопасности всех элементов ее национальной инфраструктуры. Речь идет и о государственном, и о частном секторе экономики и всего социального организма США.

На сегодняшний день все сферы жизнедеятельности общества и государства в США полностью зависят от информационных технологий и информационной инфраструктуры. В данном случае имеются в виду стабильное функционирование Интернета, телекоммуникационных сетей, встроенных функциональных автоматизированных систем (таких, например, как системы управления воздушным движением, система управления распределением электроэнергии, специализированные системы банковских счетов, персональные компьютеры[1]). Обеспечение безопасного и стабильного функционирования киберпространства, таким образом, является чрезвычайно важной и одновременно одной из самых сложных задач для американских властей.

Тема обеспечения информационной безопасности не является новой для страны, где возник Интернет. США регулярно подвергаются атакам в киберпространстве, которых обычно случается до 50.000 в день[2]. За два последних года США потратили 8 млрд. долларов на борьбу с преступлениями в Интернете[3], число которых стремительно растет[4].

Изначально в США сформировался подход двойных стандартов в отношении вопросов информационной безопасности, определявший четкий водораздел между внутренней и внешней политикой. Так, внутри страны принимались различные меры по укреплению информационной безопасности, противодействию информационному криминалу и терроризму, активно велись разработки новейших информационных технологий для военного сектора, разрабатывались сценарии информационных войн и операций. При этом на международной арене США долгое время не признавали наличия комплекса угроз информационной безопасности, включавшей в себя военную составляющую. Позиция США в этой сфере сводилась к тому, что угрозы целостности и работоспособности национальной и глобальной информационной инфраструктуры в подавляющем большинстве случаев исходят от неправомерных действий в киберпространстве, а отнюдь не от военных действий одних государств против других[5].

Исходя из этого, США приняли активное участие в разработке большого числа международных документов, в частности, таких, как:

— Конвенция по киберпреступности Совета Европы 2001 года (Convention on Cybercrime), которая содержит руководящие принципы для национальных законодательных систем и межгосударственного сотрудничества в сфере деятельности правоохранительных органов;

— «Руководящие принципы по безопасности информационных систем и сетей» (OECD Guidelines for the Security of Information Systems and Networks) Организации экономического сотрудничества и развития (ОЭСР) 2002 года, в котором акцентированы действия по борьбе с кибертерроризмом, компьютерными вирусами, хакерами и другими угрозами безопасности в информационной сфере;

— «Всеобъемлющая межамериканская стратегия кибербезопасности: многоаспектный и комплексный подход к созданию кибербезопасности» (A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity) Организации Американских Государств (ОАГ) 2004 года, согласно которой страны-члены ОАГ обязались развивать культуру кибербезопасности посредством превентивных мер в отношении кибератак, борьбы против киберугроз и киберпреступлений, защиты критической инфраструктуры и безопасности сетей[6].

При этом США отказывались от обсуждения каких-либо инициатив, направленных на выработку международных норм и правил в области международной информационной безопасности, создание международного режима использования информационных технологий, которые бы учитывали весь комплекс угроз информационной безопасности. Данная линия политического поведения сохраняется с 1998 года, когда на саммите «Россия-США» Вашингтон впервые продемонстрировал свой подход, отказавшись подписать совместное заявление глав-государств по проблеме информационной безопасности, проект которого содержал пакет превентивных мер противодействия глобальным информационным угрозам. Такой шаг можно объяснить тем, что США в своем стремлении к мировому лидерству не устояли перед соблазном использовать преимущества в информационных технологиях для политической, экономической, культурной и военной экспансии. Иначе говоря, они хотели использовать в этих целях новый вид информационное оружие[7]. Принимая во внимание тот факт, что его применение практически не ограничено существующими нормами международного права, такое оружие считалось эффективным средством достижения военных и политических целей.

Учитывая опыт двух предыдущих администраций Белого Дома, стратегия кибербезопасности, объявленная Б. Обамой в феврале 2009 года, в целом являлась продолжением выработанной ранее стратегии, однако было ясно, что методы и механизмы ее реализации, претерпят значительные изменения. Еще на этапе предвыборной гонки Б. Обама выделял в качестве основных угроз национальной безопасности использование другими странами ядерного и биологического оружия, а также кибератак[8].

После победы на выборах новый американский президент взял курс на пересмотр как внутренней, так и внешней политики США в области обеспечения информационной безопасности. Он поручил Совету по национальной безопасности в 60-дневный срок провести полный анализ существующей ситуации в области информационной безопасности страны и провести комплексную проверку усилий федерального правительства по защите информационной и коммуникационной инфраструктуры. Итогом этой работы должны были стать рекомендации по обеспечению безопасности и стабильности функционирования информационно-коммуникационной инфраструктуры США. Этот проект возглавила Мелисса Хафавей (Melissa Hathaway), Старший директор по киберпространству Программы национальной безопасности, руководитель Центра стратегических и международных исследований.

При подготовке обзора работа велась открыто и прозрачно. В процессе подготовки приняли участие представители научных кругов, фондов защиты гражданских свобод, индустрии и частного сектора. Кроме того, активно были вовлечены представители всех ветвей власти, как местных, так и федеральных. Доклад «Обзор киберполитики» (Cyberspace Policy Review), подготовленный группой экспертов, был представлен президенту США в мае 2009 года. Данный обзор содержал далеко не утешительные выводы относительно состояния информационной инфраструктуры, а также готовности военно-политических институтов США противостоять угрозам в киберпространстве. В нем отмечалось, что существующая система во многом не готова к превентивным действиям по обеспечению безопасности, реагируя лишь на свершившиеся акты кибератак[9].

Как подчеркивалось в документе, при строительстве информационной инфраструктуры США основную роль играли принципы совместимости и эффективности, при этом аспекты безопасности изначально вообще не принимались в расчет. Однако значимость вопросов безопасности резко возросла в связи с появление в XXI веке новых угроз в киберпространстве, которые представляет собой один из самых серьезных вызовов экономике и национальной безопасности страны[10]. В этой связи США столкнулись со сложной задачей. С одной стороны, государство должно было обеспечивать условия для развития инноваций, экономического процветания, свободной торговли. С другой стороны, нужно было гарантировать должный уровень защиты систем, соблюдая при этом гражданские свободы и право на неприкосновенность частной жизни.

Очевидно, что для построения системы безопасности необходимо было определить существующие для нее угрозы. Согласно аналитическим отчетам Федерального Бюро Расследований (ФБР) в 2009 году, источниками угроз критическим информационным структурам безопасности США являются следующие акторы[11]:

1. Иностранные государства. Разведывательные службы иностранных государств используют технические средства для сбора информации и проведения разведывательных операций. Все большее число государств нацелены на использование и потенциальный вывод из строя, вплоть до уничтожения, информационные инфраструктуры, включая Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и микросхемы. При этом еще в 2000 году в докладе ФБР говорилось о том, что ряд государств активно ведут исследования в области информационных войн (разрабатываются доктрины и программы, наращивается потенциал), которые могут быть направлены на разрушение коммуникаций и экономической инфраструктуры, обеспечивающие военную мощь США[12].
2. Криминальные группы, осуществляющие кибератаки с целью получения денежной прибыли.
3. Хакеры, осуществляющие проникновения в информационные системы и сети зачастую ради демонстрации своих способностей среди общности хакеров. Несмотря на то, что удаленный взлом системы требует должной подготовки и знаний, всю необходимую информацию для проведения хулиганского нападения на сайты можно найти в Интернете.
4. Хактивисты, осуществляющие атаки на Web-страницы и почтовые серверы с тем, чтобы разместить на них тексты политического характера.
5. Сотрудники компаний/«инсайдеры», обладающие подробными знаниями о компьютерных системах компании и имеющие доступ к системам, могут осуществить хищение данных, а также передать за денежное вознаграждение информацию третьим лицам. Та же угроза исходит и от персонала, работающего в компании по контрактам.
6. Террористы, действия которых направлены на: а) разрушение, вывод из строя или же использование критической инфраструктуры с целью нанесения ущерба национальной безопасности; б) ослабления экономики США; подрыва общественного стабильности и спокойствия[13].

Стоит отметить, что под определение информационного криминала подпадают действия отдельных групп или лиц, направленные на взлом систем защиты, хищение или разрушение информации в корыстных или хулиганских целях. То есть, компьютерные воры, хакеры, хактивисты и «инсайдеры» являются типичными представителями информационного криминала, и, как правило, осуществляют разовые преступления против конкретного объекта киберпространства. Таким образом, в настоящее время триадой угроз информационной безопасности по праву можно назвать возможность использования ИКТ государствами в военных целях, киберпреступность и кибертерроризм. Об этом знают и в Овальном кабинете, члены которого в полной мере осознают комплекс угроз и осуществляют действенные меры по противодействию им.

Лидерство в киберпространстве является одним из национальных приоритетов США. Для обеспечения ключевой позиции США необходимо подойти всесторонне к реализации национальной стратегии безопасности в киберпространстве, используя такие ресурсы, как дипломатия, разведка, военный комплекс, правоохранительные органы, а также инструменты в сфере экономики[14].

Американские эксперты, подготовившие обзор по кибербезопасности, отмечают необходимость проведения глубокой институциональной реформы в стране и выработки политики в области кибербезопасности. Внутренняя реформа должна реструктурировать существующие механизмы государства, гармонизировать ответственность в области кибербезопасности как в Белом доме, который должен стать лидером проекта по обеспечению информационной безопасности, так и в министерствах и ведомствах, создав четкую структуру управления, в которой возможно будет избежать дублирования функций различными ведомствами.

Так, первое лицо США, следуя рекомендациям экспертов, принял решение о создании единого Совета по национальной безопасности. При этом в Белом доме создается новый отдел, которым будет руководить Координатор по кибербезопасности, который, в свою очередь, будет являться членом Совета национальной безопасности и Национального экономического совета[15].

Кроме того, за довольно короткий период времени в целях централизации контроля за реализацией киберполитики был создан ряд новых структур по обеспечению кибербезопасности. В июне 2009 года в составе Стратегического командования Пентагона было создано военное командование по обеспечению кибербезопасности, под началом которого будет объединено самое большое число кибербойцов. В качестве приоритетной задачи была выделена защита сетей от нападений российских и китайских хакеров[16] В конце октября 2009 г. открылся Центр интеграции национальной кибербезопасности и коммуникаций (National Cybersecurity and Communications Integration Center), главной задачей которого является координация всех систем сетевой защиты страны. Технологическое оснащение Центра позволит сканировать активность в национальных сетях до нескольких миллионов раз в сутки, для того, чтобы обеспечить своевременное предотвращение киберпреступлений.

В своем выступлении по подведению итогов проведенного исследования Б. Обама в качестве первоочередных шагов в области обеспечения кибербезопасности отметил следующие:

— разработка новой всеобъемлющей стратегии по обеспечению безопасности информационно-коммуникационных сетей Америки;
— выстраивание механизмов совместных действий между государственными и местными органами власти, а также частным сектором в целях обеспечения единого и организованного подхода к ответным мерам на кибератаки (заранее вырабатывать планы по противодействию кибератакам, налаживать обмен информацией, разрабатывать систему раннего оповещения и обеспечивать скоординированные ответные меры);
— укрепление сотрудничества государственного и частного секторов, имеющее решающее значение в деле обеспечения кибербезопасности. Подавляющее большинство важнейших информационных инфраструктур в США находится в собственности либо управляется частным сектором. В этой связи сотрудничество государства и частного сектора необходимо для обеспечения технических решений в области безопасности;
— проведение передовых исследований и разработок в области ИКТ. Большие ассигнования будут выделены Администрацией на информационную инфраструктуру: строительство «умных» электросетей для более эффективного распределения электроэнергии, внедрение следующего поколения системы управления воздушным движением, а также система электронного хранения медицинской информации;
— повышение информированности и грамотности населения. Инвестиции в НИОКР, образовательные программы в школах и университетах[17].

Нужно отметить, что данные выводы не являются чем-то новым, политика предшественников нынешнего главы США во многом базировалась на данных ключевых принципах, однако не привела к должному, по мнению аналитиков, состоянию защищенности информационно-коммуникационного пространства страны. Идея создания всеобъемлющей стратегии по обеспечению кибербезопасности, озвученная Б. Обамой, начала реализовываться Дж. Бушем-младшим с января 2008 года в рамках Всеобъемлющей инициативы по обеспечению кибербезопасности (Comprehensive National Cybersecurity

Initiative). Она была направлена на трансформацию деятельности Министерства внутренней безопасности и других федеральных агентств в целях повышение эффективности противодействия вторжениям в киберпространстве[18].

Что касается сотрудничества государственного и частного секторов, то уже администрация Б. Клинтона столкнулась со сложностями в обеспечении безопасности критической инфраструктуры. Это объяснось тем, что более 85% объектов этой инфраструктуры принадлежала частным предпринимателям и использовалась ими для производства товаров и услуг[19]. Получается, что американское государство объективно не способно самостоятельно контролировать киберпространство без активного сотрудничества с частным сектором. Осознание необходимости такого партнерства нашло отражение в директиве президента Клинтона PDD-63 в 1998 году, в соответствии с которой была сформулирована так называемая «стратегия совместных усилий правительства и частного сектора в области защиты критической инфраструктуры»[20].

В дальнейшем принцип партнерства государственного и частного секторов лег в основу Национальной стратегии по обеспечению безопасности киберпространства 2003 года и Национальной стратегии физической защиты критической инфраструктуры 2003 года. В Национальной стратегии были сформулированы основные приоритеты по обеспечению безопасности киберпространства, которые фактически повторил Б. Обама в ходе своего публичного выступления, обозначив их в следующем порядке:

— национальная система реагирования на инциденты безопасности киберпространства;
— национальная программа уменьшения уязвимости и угроз безопасности киберпространства;
— национальная программа обучения и повышения осознания безопасности киберпространства;
— обеспечение безопасности государственного киберпространства;
— национальная безопасность и международное сотрудничество по обеспечению безопасности киберпространства[21].

В Национальной стратегии физической защиты критической инфраструктуры говорилось о том, что защита критической инфраструктуры страны требует координированных усилий со стороны федерального правительства, правительств штатов, частного сектора, а также всех граждан страны[22].

Ввиду глобальной взаимозависимости информационных инфраструктур государств США самостоятельно не способны обеспечить безопасность критической инфраструктуры. В этой связи одновременно с внутригосударственными преобразованиями, США намерены активизировать международный диалог в области обеспечения информационной безопасности в рамках таких международных организаций, как Организация объединенных наций (ООН), ОЭСР, «большая восьмерка», ОАГ, Международный Союз Электросвязи (МСЭ).

Несмотря на намерения проводить более открытую политику по вопросам информационной безопасности, не стоит ожидать от США кардинального пересмотра переговорной позиции по вопросам военного использования ИКТ государствами, а также выработки международного договора, который бы регулировал отношения и действия государств в киберпространстве.

Вероятнее всего, США продолжат активную работу по выработке международных мер по противодействию кибертерроризму и киберпреступности. Они будут совершенствовать основополагающие принципы по защите критической инфраструктуры, продвигая идею расширения сотрудничества в рамках международных правоохранительных групп. Их деятельность, по мнению США, способна обеспечить правопорядок в глобальном информационном поле. Вместе с тем Вашингтон будет стремиться сохранить свободу рук в вопросах проведения информационных операций и использования информационного оружия государством.

Summary: *The article is devoted to the US approach to the information security issues on national as well as international levels. The author shows the duality of the US policy concerning the existing threats to cybersecurity such as cybercrime, cyberterrorism and the use of information and telecommunication technologies by states in military and political goals. The article consists of analyses of the measures undertaken by the Administration of Barack Obama to increase the effectiveness of the cyber accidents prevention. The author draws the parallels between the cyber policies of the Administrations of Bill Clinton, George Bush and Barack Obama.*

Ключевые слова

информационная безопасность, киберпреступность, кибертерроризм, Администрация Барака Обамы

Keywords

information security, cybercrime, cyberterrorism, Administration of Barack Obama

Примечания

1. Роговский Е.А. Кибербезопасность и кибертерроризм. «США*Канада: экономика, политика, культура». — 8(404) август 2003. – С. 39
2. John Markoff, Andrew E.Kramer, U.S. and Russia Differ on a Treaty for Cybersecurity, June 28. 2009. – http://www.nytimes.com/2009/06/28/world/28cyber.html?_r=1
3. Remarks by The President on Securing our Nation's Cyber Infrastructure, The White House, Office of the Press Secretary, May 29, 2009. – http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/
4. Statement of Gregory C. Wilshusen, Director Information Security Issues, David A. Powner, Director Information Technology Management Issues, Cybersecurity. Continued Efforts Are Needed to Protect Information Systems from Evolving Threats. November 17, 2009. — http://www.gao.gov
5. US Comments on March 21st WSIS Draft Declaration and Action Plan. — http://www.state.gov/e/eb/cip/wsis/
6. A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, 8 June 2004. — http://www.cicte.oas.org/Docs/Resolucion%202004.htm
7. Коновалов А. Информационная безопасность: кто — за, кто — против?// Современная Европа. — 2003.-№2. – С. 65
8. Glen Johnson Obama warns against "fighting the last war", July 16, — http://www.usatoday.com/news/politics/2008–07–16–2873054939_x.htm
9. The Threat Working Group of the CSIS Commission in Cybersecurity for the 44th Presidency, Threats Posed by the Internet. — http://csis.org
10. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure, P. iii. — http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
11. Statement of Gregory C. Wilshusen, Director Information Security Issues, David A. Powner, Director Information Technology Management Issues, Cybersecurity. Continued Efforts Are Needed to Protect Information Systems from Evolving Threats. November 17, 2009 — http://www.gao.gov
12. Statement of Robert F. Dacey Information Security. Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures. April 8, 2003 — http://www.gao.gov
13. Statement of Gregory C. Wilshusen, Director Information Security Issues, David A. Powner, Director Information Technology Management Issues, Cybersecurity. Continued Efforts Are Needed to Protect Information Systems from Evolving Threats. November 17, 2009 — http://www.gao.gov
14. Securing Cyberspace for the 44th Presidency. A report of the CSIS Commission on Cybersecurity for the 44th Presidency, Center for Strategic and International Studies, Washington DC, December 2008, p. 1. — http://csis.org
15. Remarks by The President on Securing our Nation's Cyber Infrastructure, The White House, Office of the Press Secretary, May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/
16. Siobhan Gorman, Yochi Dreazen, — Military Command is Created for Cyber Security, 24 June, 2009, The Wall Street Journal, http://online.wsj.com/article/SB124579956278644449.html
17. Remarks by The President on Securing our Nation's Cyber Infrastructure, The White House, Office of the Press Secretary, May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/
18. Statement of Gregory C. Wilshusen, Director Information Security Issues, David A. Powner, Director Information Technology Management Issues, Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats, United States Government Accountability Office, November 17, 2009. — http://www.gao.gov
19. Леваков А. Кибербезопасность по-американски. «Известия», 5 мая 2003. — http://www.izvestia.ru
20. PDD/NSC-63, America's Critical Infrastructures, May 22, 1998. — http://www.fas.org/irp/offdocs/pdd/pdd-63.htm
21. The National Strategy to Secure Cyberspace, February 2003. — http://www.whitehouse.gov/pcipb
22. The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets. — http://www.whitehouse.gov/pcipb/physical.html