УДК 32 + 33(73)

ПОЛИТИКА США ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КИБЕРПРОСТРАНСТВА

© 2012 г. **Е.А. Роговский**[*]
Институт США и Канады РАН, Москва

В статье рассматривается стратегия глобального информационно-технологического преобладания США, в том числе роль американского правительства в международных усилиях по «глобальному руководству» и безопасности киберпространства.

Ключевые слова: *информационная безопасность, стратегия информационного преобладания, глобальное руководство, киберугроза.*

Используемые в настоящее время правительством США подходы к проблемам международной информационной безопасности тесно сопрягаются с процессом «**глобального руководства**» (*global governance, world governance*), осуществляемым с помощью глобальной сети Интернет, и предполагают известное ограничение национального суверенитета государств [24]. В соответствии с широко распространённым определением, вышеприведённый термин обозначает **процесс политического взаимодействия многих транснациональных игроков, направленный на решение какой-либо международной проблемы в ситуации отсутствия одной-единственной силы, способной такое решение обеспечить**[**].

В связи с усилением взаимозависимости как между различными сообществами, так и среди человечества в целом, «глобальное руководство» предполагает создание с помощью всемирной информационной инфраструктуры такого механизма регулирования, который был бы направлен на решение возникающих проблем сразу на глобальном уровне, т.е. не в национальных интересах какой-либо страны, а в интересах всего мира. В настоящее время вопрос о «глобальном руководстве» часто ставится в контекст глобализации тех проблем, которые длительное время не находят своего решения на региональном и национальном уровне.

Это представляется актуальным в свете выступления президента США Барака Обамы в ООН 23 сентябре 2009 г., в котором он заявил, что, политика США будет ориентироваться на смещение от доминирования к «лидерству в

[*] **РОГОВСКИЙ Евгений Александрович – кандидат экономических наук, руководитель Центра военно-промышленной политики ИСКРАН.** E-mail: Rogowsky@mail.ru

[**] См. например, определение в Википедии (http://en.wikipedia.org/wiki/Global_governance), а также работы американского нобелевского лауреата Дж. Стиглица [25; 26].

международном сотрудничестве, направленному на решение глобальных проблем» [23].

Понятие «глобального руководства и безопасности киберпространства» обычно трактуется как процесс политического взаимодействия многих транснациональных игроков, направленный на **разработку международных соглашений и стандартов безопасности и управления глобальным киберпространством.** При этом важно не упускать из вида, что США не просто принимают участие в этом многоуровневом и многогранном политическом процессе. Фактически **США – единственная страна, участвующая во всех региональных структурах экономического и политического сотрудничества – европейской ОБСЕ, американской ОАГ и азиатско-тихоокеанской АТЭК и АСЕАН*, т.е. является по существу единственной глобальной державой.** Это означает, что Соединённые Штаты располагают уникальными организационными возможностями не только для координации работы по обеспечению безопасности глобального киберпространства, но и для продвижения своих национальных и экономических интересов. Всё это предопределило широкомасштабное вовлечение в процесс «глобального руководства и безопасности киберпространства» всех ключевых федеральных ведомств США, а также множества лоббирующих негосударственных и частных организаций.

В формулировании правил и стандартов, касающихся «глобального руководства и безопасности киберпространства», а также координации их внедрения и надзора над применением, участвуют практически все ключевые структуры американской исполнительной власти – Совет национальной безопасности, Министерство торговли, Министерство обороны, Министерство внутренней безопасности, Министерство юстиции, Государственный департамент, Федеральная комиссия по связи и коммуникациям, а также Аппарат торгового представителя США. Эта деятельность полностью находится в русле государственной политики и регламентируется статусом упомянутых организаций, а также законами США и директивами президента.

В компетенции **Совета национальной безопасности** (СНБ) находятся вопросы национальной безопасности и внешней политики, требующие вмешательства президента США. В начале 2009 г. СНБ одобрил создание специального межведомственного Комитета по вопросам политики в области информационно-коммуникационной инфраструктуры. В свою очередь, в рамках этого комитета был сформирован Подкомитет по международной политике в киберпространстве (*International Sub-IPC*), в работе которого принимают участие представители всех других заинтересованных ведомств. По нашему мнению, **именно этот подкомитет формирует и координирует всю внешнюю политику правительства США в области «глобального руководства» и безопасности киберпространства**.

* В целях борьбы с киберпреступностью США также оказывают содействие в подготовке законодательства и кадров для многих африканских стран в рамках сотрудничества с такими региональными структурами как Африканский Союз, Экономическое сообщество государств западной Африки, Общий рынок восточной и южной Африки и Международная организация Франкофонии.

Участие правительственных структур в «глобальном руководстве» и безопасности киберпространства*

Министерство торговли (МТ). В координации с другими федеральными и нефедеральными структурами МТ отвечает за создание условий для производства киберсистем и развитие на их основе критически важных составляющих инфраструктуры, в том числе с помощью полномочий, предоставленных министерству законом «о военном производстве» (*Defense Production Act*). В международной деятельности МТ по кибербезопасности участвуют два его подразделения:

- *Национальная администрация по информатизации и телекоммуникациям (НАИТ)*, которую можно назвать главным консультативным органом президента США по информационной политике и телекоммуникационным вопросам. НАИТ осуществляет надзор за назначением доменных интернет-имён (в частности *.us и *.edu) и представляет правительство США в интернет-корпорации по распределению доменных имён и номеров, а сотрудники НАИТ выступают экспертами в трёх ключевых рабочих группах Международного союза электросвязи: 1) по стандартизации кибербезопасности телекоммуникаций; 2) по обмену передовым опытом в области кибербезопасности и 3) по управлению спектром радиочастот. Кроме того, НАИТ участвует в работе и других международных групп и организаций, например, упомянутого выше Подкомитета по международной политике в киберпространстве, а также региональных ОАГ и АСТЭС.
- *Национальный институт стандартов и технологий* (НИСТ) совместно с Американским национальным институтом стандартов продвигает американские инновации и укрепляет конкурентоспособность США с помощью рекомендаций в области науки, технологий и стандартов. Эксперты НИСТ участвуют и председательствуют во многих группах Объединённого технического комитета № 1 Международной организации по стандартизации, который разрабатывает стандарты, относящиеся к технологиям совершенствования информационной безопасности, в том числе методов идентификации, обработки смарт-карт, «облачным» компьютерным технологиям, биометрии и криптографии. НИСТ является региональным «директором» разработки стандартов в рамках Международной рабочей группы по интернет-инжинирингу, в том числе по шестой версии интернет-протокола (*Internet Protocol version, IPv6*), а также по группе стандартов *IEEE-802* семейства *IEEE* (Институт инженеров по электротехнике и электронике), касающихся локальных вычислительных сетей и сетей мегаполисов.

Министерство обороны (МО) отвечает за защиту своих компьютерных сетей, включая независимые двусторонние коммуникации с военными и иными структурами зарубежных стран, с помощью которых осуществляется обмен данными о компьютерной уязвимости и координация оперативной деятельности. В качестве федеральной структуры, располагающей собственной киберэкспертизой, МО сотрудничает с МВБ по вопросам защиты киберпространства и критически важных объектов инфраструктуры. В международной деятель-

* По материалу [13].

ности по глобальному управлению и кибербезопасности участвуют несколько подразделений МО. Это:

- *Управление заместителя министра по глобальной стратегии* – главная организация, ответственная за международную политику МО по вопросам киберпространства. Она содействует разработке стратегии НАТО в киберпространстве и обмену передовым опытом; участвует в составе делегации США в работе рабочих групп по стандартам кибербезопасности и обмену передового опыта, а также в работе профильных проектов ООН; разрабатывает двух- и многосторонние соглашения по военному сотрудничеству и операциям в киберпространстве; осуществляет политическое руководство другими ведомствами США, участвующими в международной деятельности, совместно с *заместителем министра обороны США по информационной политике и информационной безопасности,* разрабатывает и координирует взаимосвязи и обмен информации с международными военными партнёрами США с целью обеспечения военных операций, проводимых в компьютерных сетях;
- *Управление заместителя министра по сетевой и информационной интеграции* обеспечивает руководство и надзор над всеми используемыми в структурах министерства информационными технологиями, включая системы национальной безопасности; руководит международными информационными программами двух- и многостороннего обмена данных с международными военными партнёрами США; представляет США в структурах НАТО, утверждающих военную киберполитику, и руководит её реализацией через Управление кибероборонь НАТО; спонсирует проведение регулярных (раз в два года) международных семинаров по кибероборонe; предоставляет техническую экспертизу другим ведомствам США, участвующим в международной деятельности по кибербезопасности;
- *Директорат стратегического планирования Комитета начальников штабов* (*КНШ*) отвечает за интерпретацию национальной политики в объединённой доктрине боевых подразделений МО; организует профессиональное образование военных специалистов союзников США в соответствии с упомянутой доктриной, включая операции в киберпространстве; обеспечивает в координации с военным атташатом и Государственным департаментом работу офицеров связи, осуществляющих взаимодействие с зарубежными военными партнёрами; направляет офицеров связи для военной миссии ООН, представляет КНШ в специальном межведомственном Комитете по вопросам политики в области информационно-коммуникационной инфраструктуры.

Министерство внутренней безопасности (МВБ) отвечает за предотвращение террористических атак, защиту ключевых ресурсов и критически важных объектов инфраструктуры, а также реагирование на иные угрозы и чрезвычайные ситуации в США. К компетенции МВБ относится и безопасность международного киберпространства. В деятельности по глобальному руководству и обеспечению безопасности киберпространства участвуют многие подразделения МВБ, среди них:

- *Управление по кибербезопасности и коммуникациям* (УКБК) отвечает за обеспечение функционирования национальной системы реагирования в киберпространстве, реализацию программ управления киберрисками для защиты

критически важных объектов инфраструктуры, а также планирование и обеспечение коммуникаций федерального правительства США в чрезвычайных ситуациях. Управление принимает участие в рабочих группах по стандартам кибербезопасности и телекоммуникациям; привлекает многонациональные компании к разработке основных решений, учитывающих риски глобальной сети поставщиков; спонсирует международные академические рабочие группы, подготавливающие обзоры международных стандартов в сфере страхования информационных рисков; проводит с привлечением иностранных партнёров крупномасштабные учения по кибербезопасности, такие как *Cyber Storm,* с целью совершенствования механизмов координации и реагирования на инциденты; участвует в Глобальном форуме по компьютерной безопасности; координирует разработку стандартов и оперативных процедур реагирования для международной межправительственной сети наблюдения и предупреждения, учреждённой в 2004 г. с целью противодействия киберугрозам, кибератакам, уязвимостям, а также для укрепления системы оповещения о состоянии глобального киберпространства и потенциала реагирования на инциденты.

УКБК участвует в руководящем комитете «Меридианного процесса» – независимой международной структуры («проекта»), воплощающей руководящие принципы «восьмёрки» (*G8*) по обеспечению правительств разных стран средствами обсуждения на политическом уровне совместной работы по защите критически важных инфраструктурных объектов. УКБК является председателем «проекта» системы, контролирующей в рамках «Меридианного процесса» обмен информацией между правительствами разных стран. В составе делегаций США сотрудники УКБК участвуют в группах Комитета по телекоммуникациям АТЭС; в группах ОЭСР по информационной безопасности и конфиденциальности; в работе антитеррористического комитета ОАГ; в двух- и многосторонних связях с зарубежными странами.

Управление также проводит обучение иностранных кадров в Американском институте коммуникаций и подготовки кадров по тематике систем контроля кибербезопасности и проводит экспертизу связанных с кибербезопасностью программ НАТО по планированию гражданских коммуникаций.

Секретная служба США отвечает за расследование преступлений, связанных с финансовой инфраструктурой США, включая компьютерные мошенничества, киберпреступления а также электронные преступления иных типов. Служба командирует своих сотрудников в Министерство юстиции для координации криминальных расследований с Интерполом; расследует международные киберпреступления с помощью специальных агентов, в том числе через Европейское бюро электронных преступлений; обеспечивает подготовку сотрудников для этого бюро и Международной академии правозащиты. Сотрудники этой службы участвуют в совещаниях министров юстиции и в деятельности антитеррористического комитета Организации американских государств.

Министерство юстиции (**МЮ**) – главное правоохранительное ведомство правительства США, ответственное за расследования нарушений законодательства, связанных с киберпространством. Президентская директива «Об идентификации и приоритетах критически важных инфраструктурных объектов, а

также их защите» предписывает МЮ совместно с МВБ выявлять и расследовать киберугрозы и кибератаки. Кроме того, эта директива предписывает МЮ и другим федеральным агентствам сотрудничать с зарубежными странами и международными организациями с целью укрепления защиты критически важных инфраструктурных объектов и ключевых ресурсов США. МЮ принимает участие в работе упомянутого выше Подкомитета по международной политике в киберпространстве. В международной деятельности по обеспечению кибербезопасности участвуют многие подразделения МЮ, среди них:

- *Отдел по борьбе с компьютерными преступлениями и защите интеллектуальной собственности (ОКПИС)* отвечает за преследование совершивших электронные преступления граждан США и иностранцев, участвует во внешнеполитической деятельности США, связанной с вопросами киберпреступности, включая «право свободы слова» и иные юридические вопросы. ОКПИС руководит деятельностью экспертов в работе подгруппы G8 по высокотехнологическим преступлениям, а также в постоянно действующей глобальной контактной сети; председательствует в исполкоме Конвенции Совета Европы по киберпреступности.

ОКПИС готовит кадры для расследования киберинцидентов и преследования преступников для международных и региональных организаций, для африканских стран, ведущих борьбу с киберпреступностью, а также для прочих национальных организаций, проводит межведомственные встречи по вопросам координации подготовки международных кадров, оказывает чрезвычайную помощь национальным и зарубежным государственным организациям, а также таким межгосударственным организациям, как Интерпол, в получении из зарубежных стран электронных доказательств; взаимодействует с Директоратом ЕС по вопросам выявления киберпреступлений, международной системы подготовки кадров по киберпреступности и другим политическим вопросам, относящимся к интернет-корпорации по распределению доменных имён и номеров. ОКПИС готовит также законодательные предложения и комментарии на законодательные предложения по вопросам международной киберпреступности, а также критические замечания на законопроекты других стран.

- *Киберподразделение ФБР* является ведущей федеральной структурой по расследованию нарушений законов США, связанных с киберпреступлениями, включая криминальные интернет-вторжения, защиту детей от нежелательной онлайновой информации, защиту интеллектуальной собственности и кражу персональных данных. ФБР устанавливает двух- и многосторонние связи с иностранными странами с целью кооперации в расследовании киберпреступлений; председательствует в рабочей группе по киберпреступлениям «Стратегического союза» – многосторонней международной организации по совершенствованию кооперации правоохранительных органов; руководит международной рабочей группой в рамках инициативы противодействия производству и распространению детской порнографии и агрессивным онлайновым хакерам («хищникам»).

ФБР командирует своих сотрудников в иностранные правоохранительные органы для содействия расследованию нарушений кибербезопасности, курирует региональных интернет-регистраторов и провайдеров, готовит кадры для расследований киберпреступлений. руководит деятельностью «Объединённой

национальной группы киберрасследований», которая объединяет разведывательные и правоохранительные органы и предназначена для расследования, предсказания и предотвращения кибертерроризма, кибершпионажа и киберпреступлений.

- *Подразделения национальной безопасности* МЮ США – ПНБ МЮ США. Противодействие кибертерроризму входит в число основных задач этих подразделений Минюста. С целью совершенствования механизма реагирования на киберинциденты, а также для координации общих усилий они участвуют в широкомасштабных учениях по кибербезопасности, проводимых совместно с международными партнёрами, консультируют подготовку докладов в рамках глобальной инициативы «Свобода Интернета»; участвуют в семинарах ООН по правовым и техническим аспектам противодействия терроризму с использованием Интернета; участвуют в работе специального подкомитета по международной политике в киберпространстве.
- *Центральное национальное бюро Интерпола (ЦНБН)* представляет Соединённые Штаты в качестве члена Интерпола и является контактной организацией для федеральных структур США, властей штатов, местных органов, а также иных правоохранительных органов для осуществления международного обмена информацией по криминальным расследованиям.

Государственный департамент имеет множество обязанностей, связанных с киберпространством и отвечает за формулирование, координацию и надзор над всеми аспектами внешней политики, связанными с международными коммуникациями и информационной политикой, включая осуществление полномочий определения позиции США и участие в переговорах с иностранными правительствами и международными организациями. Государственный департамент отвечает также за координацию и надзор исполнения всех основных научно-технических соглашений; возглавляет федеральные усилия по укреплению международной кооперации по безопасности киберпространства; сотрудничает с МВБ по обеспечению безопасности киберпространства; участвует в работе упомянутого выше специального международного Подкомитета по международной политике в киберпространстве. В международной деятельности по обеспечению кибербезопасности участвуют многие подразделения Государственного департамента, среди них:

- *Бюро по вопросам экономики, энергетики, бизнеса, международных коммуникаций и информационной политике* отвечает за международные коммуникации и информационную политику. Руководит формированием и координацией позиции США на конференциях и ассамблеях Международного союза электросвязи (МСЭ); возглавляет делегации США в трёх ключевых рабочих группах: 1) по стандартам кибербезопасности и телекоммуникаций; 2) по обмену передовым опытом (руководит подготовкой её рекомендаций в области доступных инструментов кибербезопасности); 3) по тематике исследований, связанных с кибербезопасностью радиочастотного спектра; участвует в ежегодных встречах Совета МСЭ, а также в работе его экспертных групп по вопросам идентификации проблем глобальной кибербезопасности и подготовке мер реагирования.

Бюро проводит ежегодные Диалоги информационного общества с Европейской комиссией по развитию телекоммуникаций и информационных техноло-

гий; участвует в деятельности независимого Форума по управлению Интернетом; сопредседательствует совместно с Управлением по демократии, правам человека и труду Госдепа США в рабочей группе по «сетевой свободе», целью которой является продвижение свободных потоков информации и свободы выражения мнений в Интернете.

Бюро также возглавляет делегацию США на регулярных (раз в два года) встречах руководящей группы по безопасности и развитию Комитета по телекоммуникациям (APEC); на совещаниях группы ОБСЕ по информационной безопасности и конфиденциальности, разрабатывающей политику поддержания доверия, информационной безопасности и личной конфиденциальности (прайвеси); на собраниях профильной группы ОАГ, обсуждающей региональные вопросы, ранее находившиеся в компетенции МЭС (включая кибербезопасность).

- *Отдел по киберпроблемам Бюро по разведке и исследованиям* Государственного департамента США ответственен за проведение разведывательной аналитической работы и координацию международных контактов по вопросам кибербезопасности. Он ведёт переговоры по одобрению резолюций ООН, в частности тех, которые связаны с борьбой против использования информационных технологий в криминальных целях, с созданием глобальной культуры кибербезопасности, с защитой критически важных инфраструктурных объектов, в том числе с усилиями национальных государств по защите критически важных составляющих информационной инфраструктуры. Эксперты отдела участвуют в делегациях США на совещаниях АСЕАН, посвящённых политике в области кибербезопасности и таким вопросам международной безопасности, как использование Интернета террористами; представляют США в группе правительственных экспертов ООН; руководят работой американской делегации в ОБСЕ, спонсируют проведение семинаров и экспертиз по вопросам защиты критически важных объектов инфраструктуры и кибербезопасности; участвуют в профильных конференциях и семинарах «Меридианного процесса», а также в двух- и многосторонних связях с зарубежными странами; готовят аналитические материалы по вопросам международной кибербезопасности; координируют представительство Государственного департамента на различных профильных форумах. Отдел разрабатывает и координирует политику защиты интересов безопасности США в Европе, в том числе в отношении НАТО, включая политику кибероборонь НАТО.
- *Бюро Госдепартамента по делам международного правоприменения международного законодательства против наркотиков* тоже отвечает за координацию программ борьбы с киберпреступностью. Это бюро руководит делегацией США в подгруппе по высокотехнологичной преступности «восьмёрки» (*G8*), а также работой по борьбе с киберпреступностью в рамках ОАГ; способствует применению Конвенции ООН против транснациональной организованной преступности в качестве альтернативного инструмента борьбы с киберпреступностью; участвует в Подкомитете по международной политике в киберпространстве.
- *Отдел Госдепа по делам европейской политики и безопасности* разрабатывает и координирует политику защиты интересов безопасности США в Европе, в том числе в отношении НАТО, включая политику кибероборонь блока.

Международное бюро Федеральной комиссии по связи (ФКС) – независимое федеральное агентство, ответственное за регулирование внутренних и международных радио, телевизионных, проводных, спутниковых и кабельных коммуникаций. Активно участвует в работе упомянутого выше специального подкомитета и консультативной группы советников по стандартизации телекоммуникаций; участвует в составе делегаций США в рабочих группах Международного союза электросвязи (МСЭ), а также заседаниях соответствующих комитетов и групп ОАГ и ОЭСР.

Управление торгового представителя США отвечает за разработку и координацию внешнеторговой политики США, а также за ведение торговых переговоров с другими странами и многосторонними организациями, участвует в работе специального Подкомитета по международной политике в киберпространстве, предоставляет услуги технической экспертизы и консультации другим федеральным агентствам, участвующим в международной деятельности этого подкомитета; возглавляет деятельность США по борьбе с контрафактной продукцией, по применению международных стандартов защиты прав собственности в цифровом пространстве; является членом Комитета по международной политике Американского национального института стандартов (ANSI), а также Международной организации стандартов.

Приведенная организационная структура участия американского государства в «глобальном руководстве» и безопасности киберпространства, по нашему мнению, позволяет заключить, что в целом она создаёт для администрации Обамы возможности последовательного проведения в этой области разносторонней многоцелевой политики, соответствующей национальным интересам США.

Политика администрации

В «Стратегии национальной безопасности Соединённых Штатов», обнародованной в мае 2010 г. [21], содержится ряд существенных нововведений, которые позволяют говорить, что политика Соединённых Штатов в сфере национальной безопасности претерпела значительные изменения. Так, теперь в борьбе как с внешними, так и с внутренними угрозами американская администрация собирается применять силу более осмотрительно – «используя вместо молотка скальпель». В этой связи в стратегии «предлагается интегрировать основные инструменты американской мощи: дипломатию, военную силу, экономические инструменты, разведку, силы обеспечения внутренней безопасности». В отношении информационных технологий в стратегии отмечается, что они «обеспечивают военное превосходство США, но делают американскую гражданскую экономику чрезвычайно уязвимой» [1], слишком «реактивной», как в своё время отметил бывший глава ФРС Алан Гринспен. В определённом смысле это означает, что широчайшее распространение этих технологий в американской экономике во многом истощает ресурсы её надёжности и, следовательно, подрывает её устойчивость, что следует рассматривать в качестве одной из приоритетных проблем национальной экономической безопасности страны.

Это стало причиной нарастания озабоченности мирового сообщества, тесно связанной с возможностями применения новых технологий в целях, не совместимых с задачами обеспечения международной стабильности. Уязвимость ис-

пользуемой информационной инфраструктуры, с одной стороны, и уникальные возможности наиболее передовых информационных технологий – с другой, способствовали появлению принципиально нового вида оружия – информационного, а также связанных с его применением информационно-технологических угроз международной безопасности. В список важнейших угроз здесь следует занести враждебное использование информационно-коммуникационных технологий в отношении критически важных элементов информационной инфраструктуры другого государства в политических, в том числе военных целях, а также преступную и террористическую деятельность в киберпространстве.

В этом контексте можно считать, что сфера международной информационной безопасности распространяется за границы киберпространства и включает такую угрозу, как целенаправленное создание и использование доминирующего положения той или иной страны в глобальном информационном пространстве в ущерб интересам безопасности других государств. Источником этой угрозы является неравномерность в развитии информационных технологий в различных государствах, а также существующая тенденция к увеличению «цифрового разрыва» между развитыми и развивающимися странами. Некоторые государства, располагающие мощными системами сбора и обработки данных, добиваются в глобальной сети доминирующих позиций и под лозунгом «распространения западных демократических ценностей» претендуют на свободный доступ к информационным ресурсам других суверенных стран.

При этом круг возможностей «недружественного» применения все более совершенных информационных технологий расширяется намного быстрее, чем политики и законодатели успевают этот процесс осмыслить. В этой сфере, по мнению авторитетных специалистов (например, М. Хатавей, еще совсем недавно бывшей «киберцарицей» в администрации президента Б. Обамы) сегодня уже даже в развитых странах «оборонительные технологии» просто не поспевают за возникающими угрозами. Более того, в этой сфере создавать новые (наступательные) угрозы зачастую проще (и многократно дешевле), чем развивать оборону, адекватную существующим реальным угрозам [13].

С этой точки зрения сама концепция национальной безопасности США может строиться не на основе достаточности средств защиты от существующих угроз и даже не путём отражения киберопасности паритетными встречными угрозами, а с помощью стратегии абсолютного информационно-технологического преобладания над потенциальным противником, а именно:

1) достижением проницаемости информационного пространства потенциальных противников, достаточной для заблаговременного выявления угрозы своим интересам;

2) опережающим «изобретением» новых информационных угроз, неприемлемых для потенциальных противников;

3) надёжной защитой собственной информационной инфраструктуры.

Этим составляющим стратегии абсолютного информационно-технологического преобладания соответствуют четыре направления политики США в киберпространстве:

1. Сохранение американского контроля над Интернет-корпорацией по назначению доменных имён и номеров;

2. Борьба за свободу Интернета, в том числе формулирование и внедрение международных стандартов, так называемого «ответственного поведения» пользователей киберпространства;

3. Противодействие глобальному кибертерроризму и защита критически важных составляющих инфраструктуры;

4. Разработка доктрины и стратегии применения кибероружия в военных целях.

Остановимся на краткой характеристике этих направлений современной международной киберполитики США.

1. Как известно, в 1998 г. Корпорация по назначению доменных имён и номеров (КНДИН) и Министерство торговли США подписали Меморандум о взаимопонимании [19]. Интересно отметить, что поначалу правительство США воспринимало Интернет исключительно как инструмент развития национальной (американской) экономики и намеревалось полностью устраниться от управления системой назначения доменных имён.

В дальнейшем администрация Клинтона, всемерно содействовавшая распространению в мире интернет-технологий, пришла к заключению, что они становятся мощным фактором международной политики, и решила продолжить регулирование Интернета со стороны американского государства до тех пор, пока все пользователи сети «не будут готовы предпринимать ответственные, совместно принятые, законные действия, которые обеспечат поддержание стабильного функционирования системы». При этом правительство США опиралось на такое управление системой доменных имён, когда обязательные стандарты (правила) устанавливались не путём издания законов, а с помощью контрактов (и иных соглашений), заключаемых КНДИН с частными регистраторами доменных имён. Наряду с учредительными документами КНДИН, определяющими его функции, упомянутый Меморандум о взаимопонимании, наделяет правительство США определёнными властными полномочиями [3].

То, что Соединённые Штаты не собираются отдавать бразды правления Интернетом ни ООН, ни ЕС, ни какой-либо другой международной или национальной организации, было подтверждено в известном письме государственного секретаря Кондолизы Райс и министра торговли Карлоса Гитерреза, которое незадолго до начала Всемирного саммита по Информационному обществу (*WSIS*) 2005 г. в Женеве было направлено министру иностранных дел Великобритании Джеку Стро. В этом документе было жёстко заявлено, что «структура управления Интернетом и поддержание его стабильности являются жизненно важными интересами США» и что «необходима поддержка существующей организации управления Интернетом, которая доказала свою состоятельность и способность обеспечить его развитие» [8].

2. США выступают за свободу Интернета, за расширение его доступности, за снятие ограничений на его использование, «помогают людям всего мира пользоваться в открытом Интернете универсальными правами», выступают «за предоставление всем людям площадки для выражения своего мнения»... но всё это только до тех пор, пока они «ведут себя в киберпространстве ответственно», т.е. ***пока они соблюдают некие нормы поведения и не нарушают законы США***. Это суть так называемой «цифровой дипломатии» Госдепартамен-

та США, которую государственный секретарь Х. Клинтон изложила в своих выступлениях в 2010 и 2011 гг. [6; 7]. Так называемых «***плохих парней***», препятствующих «свободному» использованию Интернета или пользующихся им «неправильно», – интеллектуальных пиратов, хакеров, кибертеррористов, партнёров компании «Викиликс» и прочих нарушителей норм ответственного поведения в киберпространстве, – ***необходимо выявлять и глобально преследовать***, независимо от их гражданства, а также от особенностей юрисдикции государства, в котором они пребывают. Более того, «страны или отдельные граждане, причастные к информационным атакам, должны понести суровое наказание и международное порицание, Интернет объединяет практически весь мир, атака на сеть одного государства может быть атакой на всех».

В мае 2011 г. федеральное правительство США обнародовало уникальный документ – «Международную стратегию развития киберпространства» [15], в котором вышеизложенная позиция США в отношении защиты киберпространства была скреплена подписью президента Б. Обамы.

3. Предотвращение и сдерживание террористических кибератак, защита критически важных объектов инфраструктуры и реагирование на иные угрозы и чрезвычайные ситуации в США относятся к компетенции Министерства внутренней безопасности, которое вместе с другими федеральными агентствами, международными организациями и бизнесом отвечает и за укрепление безопасности международного киберпространства. Единая стратегическая позиция МВБ содержится в специальном документе, опубликованном в конце 2011 г. [5]... и состоит в том, что критически важные объекты информационной инфраструктуры необходимо защитить уже сегодня, пока будущая киберэкосистема ещё только формируется. В этом документе МВБ обращается внимание на то, что при обеспечении безопасности критически важных элементов национальной информационной инфраструктуры необходимо добиться эффективного партнёрства с частным сектором и предоставлять ключевым лидерам частных компаний оперативный доступ к сведениям о появляющихся угрозах, чтобы бизнес (если только он не относится к «плохим парням») успевал принять соответствующие меры.

4. Одним из наиболее значимых событий 2011 г. стало активное подключение Пентагона к защите американских интересов в киберпространстве! В том году были разработаны Доктрина и Стратегия применения кибероружия, которое по существу превращается в самостоятельный силовой фактор современной международной политики.

США признали, что инфраструктура страны оказалась «прискорбно незащищённой» и очень уязвимой для разнообразных кибератак. Обобщая данные о кибератаках, бывший руководитель Агентства национальной безопасности США и директор Национальной разведки США адмирал М. МакКоннелл предупреждал, что в отношении военных информационных ресурсов вопросы кибербезопасности стоят в США особенно остро. В статье, опубликованной в газете «Вашингтон пост», он высказался достаточно жёстко: «США уже находятся в состоянии информационной войны и проигрывают её» [18]. Более того, круг «инновационных возможностей недружественного применения» ИТ-технологий расширяется намного быстрее, чем законодатели успевают это осмыс-

лить, и даже в США «оборонительные технологии» просто не поспевают за возникающими угрозами [2].

Поскольку скорость «полёта» информации в Интернете сопоставима со скоростью света, для отражения кибернападения времени остаётся очень мало (здесь важны миллисекунды). Человек принять осмысленное решение за этот краткий миг просто не в состоянии. Реагировать должны компьютеры, заранее оснащённые соответствующими программами. Для мониторинга и идентификации несанкционированного кибервторжения, определения источника атаки, а также получения доказательств, которые будут основанием дипломатического, юридического или даже военного преследования, необходимо разработать быстродействующую систему «сверхраннего» предупреждения.

Однако в этом случае может остаться не решённой проблема направления «ответного удара». Если ракета летит из определённого заранее разведанного места расположения, то компьютерный вирус появляется фактически «ниоткуда». Поэтому из-за огромных объективных трудностей *идентификация источника кибератаки в глобальной сети может потребовать времени, несопоставимого с продолжительностью самой атаки*, и затянуться на несколько месяцев или вообще не дать никаких результатов. Кроме того, даже после идентификации источника кибератаки, его нельзя автоматически считать целью для нанесения ответного удара, поскольку этот источник может принадлежать не государству, а какой-либо террористической группе, к которой Соединённые Штаты не могут даже предъявить требования о возмещении ущерба, поскольку у неё нет никакого имущества. Более того, не всегда ясно, какой именно киберинцидент является военной атакой. Многие из современных «несанкционированных проникновений» в компьютерные сети скорее являются шпионажем, чем актом войны. Чаще всего кибератаки исходят из серверов, находящихся в собственности транснациональных корпораций в нейтральных странах.

По мнению заместителя министра обороны США У.Дж. Линна III в противодействии кибератакам концепция ответного удара, предполагающая нанесение противнику «неприемлемого возмездия» не должна быть главным элементом стратегии сдерживания. ***Главными в такой стратегии должны стать заблаговременные усилия, способные сделать такие атаки бессмысленными, безрезультатными, неэффективными*** [16].

В основу современной доктрины кибероборонь США заложена стратегия адекватного реагирования на кибератаки, которая должна предоставлять Пентагону необходимые «возможности и операциональную гибкость». Более того, «американские военные должны отвечать на кибернападение сразу после того, как оно произошло, и по возможности даже до того, как оно достигло своей цели». Как нам представляется, в этом случае компьютерные системы, образующие эшелоны кибероборонь тех или иных информационных сетей, должны быть подобны «активной броне», отражающей подлетающий снаряд с помощью встречного микровзрыва. Иначе говоря, реакция такой «активной компьютерной брони» на зафиксированную кибератаку должна опираться на возможности поражения, если не самого противника, то по крайней мере запущенного им вируса. Фактически это означает, что система кибербезопасности США (подобно ракетно-ядерному щиту) должна носить не только оборонительный, но и наступательный характер.

Именно таким соображениям и соответствует внедряемая Министерством обороны трехслойная система кибероборонь. Её первые два слоя опираются на передовой опыт коммерческих структур: на соблюдение обычной компьютерной антивирусной гигиены, на применение чувствительных сенсоров, выявляющих и классифицирующих кибератаки, а также на своевременное обновление программного и аппаратного обеспечения, восстанавливающего работоспособность подвергшейся атаке системы. Задача этих первых двух эшелонов кибероборонь – снизить результативность кибернападения.

Но по мнению американских военных специалистов, в условиях кибервойны строить системы пассивной обороны недостаточно, решающее значение здесь приобретает скорость и маневренность *наступательных операций*. Поэтому Пентагон создаёт третью линию обороны, которая опирается на (весь!) разведывательный потенциал правительства, и призвана обеспечить «высокоспециализированную активную оборону», в частности, распознавание источника атаки («лишение противника анонимности») и его нейтрализацию.

Сказанное позволяет заключить, что основные риски (угрозы), Пентагон осознал и уже заложил их в основу новой концепции организационной структуры кибероборонь США, включающей:

- создание командования войсками кибероборонь, его оснащение необходимым оборудованием и подготовку военнослужащих;
- внедрение многоступенчатой системы активной обороны;
- использование потенциала вооружённых сил для содействия другим федеральным ведомствам в защите правительственных информационных сетей и критически важных элементов национальной инфраструктуры;
- создание совместно с союзниками США системы коллективной кибербезопасности;
- организацию финансирования разработок, направленных на быстрое развитие дополнительных возможностей кибероборонь.

Успешное выполнение военных, разведывательных и деловых (бизнес) операций МО сегодня в значительной степени зависит от киберпространства. Однако помимо множества новых возможностей, предоставляемых киберпространством, военное ведомство столкнулось здесь и со значительными трудностями. Эти проблемы, а также возможности их решения рассмотрены и оценены в «Стратегии Министерства обороны по операциям в киберпространстве» [11], которая появилась в июле 2011 г. Суть стратегического подхода к этим вопросам хорошо отражают два следующих положения: «Угрозы кибербезопасности представляют собой одну из наиболее серьёзных проблем национальной безопасности, общественной безопасности, а также экономики, с которыми столкнулась наша страна» (из «Стратегии национальной безопасности США-2010»), и «Неудача МО в обеспечении безопасности своих информационных систем в киберпространстве является фундаментальным риском в отношении способности выполнять функции обороны страны, как сегодня, так и в будущем» (из «Военного обзора-2010») [4].

В «Стратегии Министерства обороны США по операциям в киберпространстве 2011» утверждается, что законы о вооруженном конфликте, которые регламентируют уровень соответствующих военных операций в условиях явной агрессии зарубежной страны, должны также распространяться и на киберпро-

странство и кибероперации. В этом документе обозначены следующие пять новых стратегических инициатив:

1. В контексте задач организации, подготовки и оснащения военнослужащих рассматривать киберпространство как операционную среду с тем, чтобы Минобороны могло пользоваться преимуществами в этой среде своего потенциала;
2. Разработать и внедрить для защиты (информационных) сетей и систем МО США новую концепцию оборонных операций;
3. Подготовить в партнёрстве с другими правительственными ведомствами и частным сектором общеправительственную стратегию кибербезопасности;
4. Сформировать надёжные взаимосвязи с союзниками и международными партнёрами США для укрепления коллективной кибербезопасности;
5. МО США должно с помощью киберспециалистов исключительно высокой квалификации, а также посредством быстрых технологических инноваций обеспечить проведение в этой области самых передовых исследований и разработок.

Приведённые стратегические инициативы фактически заменяют «Всестороннюю национальную инициативу по кибербезопасности», подготовленную администрацией Дж. Буша-мл. ещё в 2006 г. и рассекреченную администрацией Б. Обамы в 2009 г. [28]. Фактически эти пять инициатив образуют «дорожную карту» для проведения оборонным ведомством США эффективных операций в киберпространстве по защите национальных интересов и достижения целей национальной безопасности. Каждая из инициатив носит особенный характер и тем не менее необходимо связана с четырьмя другими. Деятельность по реализации этих инициатив будет способствовать реализации Стратегии МО в целом и формированию новых подходов в реализации других инициатив.

При реализации новой стратегии Министерство обороны будет использовать те возможности, которые предоставлены ему в киберпространстве для защиты собственных сетей и систем от внедрения и враждебной деятельности, для укрепления кибербезопасности на межведомственном и международном уровне, а также на уровне критически важных партнёров в промышленности, для разработки новых надёжных возможностей проведения операций в киберпространстве, а также нового партнёрства в этой сфере. Эта стратегия позволит МО защитить интересы США в киберпространстве настолько, насколько это нужно, чтобы Соединённые Штаты, а также их союзники и партнёры могли продолжать получать выгоду от инноваций информационной эпохи.

Стратегию МО США по операциям в киберпространстве прокомментировал упомянутый выше заместитель министра обороны США У. Дж. Линн III, который в сентябре 2011 г. опубликовал в журнале «Форин афферз» статью «Кибестратегия Пентагона год спустя. Защищаясь от следующей кибератаки» [17].

В этой статье У.Дж. Линн, в частности, подчёркивает, что кибератаки станут существенным компонентом будущих конфликтов. Сегодня более тридцати стран мира уже имеют или создают в своих вооружённых силах специальные киберподразделения. И конечно, просто невозможно поверить, что все они ограничат свои потенциальные возможности только обороной. Более того, сосредоточение информационных технологий в военной и в гражданской сферах американского общества делает их целями для кибератак противника. Линн

особо подчёркивает, что ***сегодня США находятся в самом начале «стратегического сдвига», ориентированного на придание киберугрозам стратегической значимости***.

До настоящего времени вторжения в большинстве случаев осуществлялись с такими целями, как кража интеллектуальной собственности из коммерческих сетей или шпионаж в правительственных структурах. Сегодня киберугрозы становятся намного серьёзнее и в контексте своей разрушительной силы, и в контексте скорости распространения информации в современном глобализованном мире. Существенно более разрушительные инструменты создаются практически каждый день, но широко не используются (поскольку наиболее ярые противники такими технологиями пока не располагают). Но такая ситуация долго продолжаться не может. «Намерения» и «возможности» скоро соединятся, – все, кто хотел бы нанести США ущерб, получат такую возможность. Можно сказать, что, задача борьбы с хакерами и кибертеррористами расширяется до военных формулировок предотвращения и отражения враждебных действий (фактически агрессии) в киберпространстве. Соединённые Штаты должны к этому подготовиться и успеть создать сильную оборону.

20 октября 2011 г., командующий Киберкомандованием США генерал армии К. Александер, выступая на проходящей в Балтиморе конференции Международной ассоциации по системам безопасности, заявил, что находящаяся на рассмотрении КНШ новая доктрина установит правила реагирования на атаки в киберпространстве [20]. Эта доктрина определит и условия, при которых военные смогут применять против киберугроз специфические наступательные меры, и то, какими именно такие меры могут быть. Доктрина конкретизирует опубликованную в июле 2011 г. «Стратегию Министерства обороны США по операциям в киберпространстве» [11], а также упомянутую выше «Международную стратегию развития киберпространства», утвержденную президентом Обамой в мае 2011 года.

Киберкомандование должно разработать руководящую инструкцию для своей киберармии (фактически «Устав киберармии»), которая определит, как именно она должна оперировать в киберпространстве, и начать соответствующую подготовку военнослужащих. Среди вопросов, которые МО США рассматривает в связи с работой над новой военной доктриной, есть и юридические вопросы о правовой основе войны в киберпространстве. Как известно, применение наземного оружия в вооружённых конфликтах регламентируется соответствующими законами; применение оружия в киберпространстве тоже должно регламентироваться законами. Проблема, однако, состоит в том, как трансформировать законы, регламентирующие применение оружия в физическом пространстве, для киберпространства, которое стало сейчас пятой сферой возможных военных конфликтов (после земли, моря, воздуха и космоса).

В этом контексте генерал К. Александер обратил внимание на необходимость определения того, что считать обоснованным пропорциональным ответом на кибератаку. Закон о вооружённом конфликте санкционирует обоснованное и пропорциональное применение силы (оборону) против физических атак, происходящих из другой страны. Распространяя эту логику на киберпространство, он заявил, что остаётся неясным, создаются ли тем самым полномочия «сбивать» компьютерные сети, если они захвачены вражескими кибервоинами.

И если создаются, то всё равно остаётся без ответа вопрос, кто именно получает такие полномочия – ФБР, АНБ, МО, провайдер интернет-услуг или кто-то ещё. Политики, со своей стороны, могут сказать: «Вы уже и так уполномочены это делать».

По мнению генерала К. Александера, на эти и все иные подобные вопросы должны ответить различные нормативные документы – военная доктрина, законы, инструкции и прочие правила реагирования, на основе которых военные сформируют программы подготовки киберсолдат. Действующие в настоящее время программы сфокусированы в основном на способах защиты сетей МО, однако генерал Александер ожидает, что сфера такого рода подготовки расширится и будет включать «весь спектр операций» против выявленных киберугроз. Он подчеркнул важность такой подготовки, учитывая нарастающее количество и опасность киберугроз: «Мы должны быть готовы к тому, что национальные государства, группы негосударственных игроков и хакеров создают для своих кибератак всё более изощрённые и угрожающие инструменты, а потому внедряемые нами структуры безопасности должны ориентироваться на будущее» [20].

Основное содержание ***доклада Минобороны***, посвященного политике в киберпространстве и представленного Конгрессу США в ноябре 2011 г., сформулировано в утверждении: «**Соединённые Штаты резервируют за собой право применения военной силы в ответ на любую значительную кибератаку, направленную против американской экономики, правительства или военных**... По приказу мы будем отвечать на враждебные атаки в киберпространстве, так же как мы должны реагировать на все иные угрозы нашей стране. Мы резервируем право использовать для защиты нашей страны, наших союзников и партнёров, а также наших интересов все необходимые средства – дипломатические, информационные, военные или экономические» [10].

В докладе отмечается, что операции в киберпространстве должны проводиться в режиме, подобном традиционным военным операциям. Вместе с тем признаётся отсутствие исторических прецедентов «традиционной военной деятельности в киберпространстве», а также отсутствие театра (и опыта проведения) такого рода военных действий в период до изобретения современных информационных и коммуникационных технологий, таких как Интернет. Поэтому вопрос о том, могут ли такие операции проводиться в соответствии с той же политикой, теми же принципами и правовым режимом, которые присущи «кинетическому оружию» и «традиционным военным операциям», требует разрешения.

Далее отмечается, что использование наступательных операций в киберпространстве допустимо в те моменты времени, когда такие операции рассматриваются в качестве наиболее дешёвого и эффективного способа военной нейтрализации идентифицированных угроз.

Подчёркивается, что в отношении наступательных операций в киберпространстве, как и в отношении любого иного применения силы должна применяться ставшая законом резолюция 1973 г. «О военной силе» (*Public Law 93-148*). Признаётся, что осуществление наступательных операций в киберпространстве в определённом смысле является наиболее эффективным способом противодействия угрозам и защиты ВС США и их союзников, включая те спосо-

бы, когда в операциях принимает участие правительство США или когда его роль явно обозначена.

Классификация кибератак и уровня соответствующего ответа будет определяться следующими оценками: причинение кибератакой «смерти», «ущерба», «разрушения» или «высокого уровня нарушения функций объекта». В соответствии с этой градацией значимое событие может повлечь существенный военный ответ, учитывающий размеры нанесённого «ущерба».

В декабре 2011 г. Конгресс США санкционировал допустимость военных наступательных операции в киберпространстве [9], предоставив военным официальное разрешение на применение таких операций в необходимых масштабах. Такое разрешение содержится в з*аконе «О финансировании обороны в 2012 г.*». Раздел 954 этого документа гласит: «*Конгресс подтверждает, что МО имеет возможности и по указанию президента может провести наступательные операции в киберпространстве для защиты страны, её союзников и интересов*» [22].

В этом свете весьма убедительно выглядит последний ***доктринальный документ*** Министерства обороны США «Продолжение глобального лидерства США: приоритеты обороны в XXI веке» (январь 2012 г.), подтверждающий, что Соединённые Штаты вместе со своими союзниками и партнёрами будут и дальше возглавлять международные усилия по обеспечению доступа и использованию таких глобальных ресурсов, как океаны, атмосфера, космос, а также Интернет, как путём укрепления международных норм (стандартов) «ответственного поведения», так и путём поддержания адекватного военного потенциала [27].

По определению Министерство обороны, «превосходство в киберпространстве» означает состояние, когда США и дружественные им силы располагают полной свободой деятельности в киберпространстве, тогда как силы противника такой свободой не располагают. И достигнуто это превосходство может быть за счёт опоры на уникальный потенциал глобального информационного мониторинга, созданный в начале XXI века на волне борьбы с терроризмом. Фактически **правительство США поставило задачу предотвратить использование глобальной информационной инфраструктуры против интересов США. Это означает лишение конкурентов** (не только противников, но и партнёров) даже мизерной **возможности сохранять свои коммерческие, научно-технические, политические и прочие секреты, что эквивалентно отрицанию права всех стран мира на сохранение информационного суверенитета.**

Особо следует подчеркнуть, что с военной точки зрения Минобороны противостоит не столько хакерам, сколько внешней киберагрессии. Поэтому в документах высокого уровня очень важна явная идентификация неприятеля, что и было сделано в 2011 г., когда впервые главным киберпротивником США был назван Китай [11].

Судя по интервью, которое дал один из наиболее авторитетных специалистов ФБР по компьютерной преступности Ш. Генри (размещено в марте 2012 г. на сайте ФБР) [29], в настоящее время серьёзную угрозу для США представляют не «свободные юнцы-хакеры», а следующие три источника кибератак:

– организованные преступные группы, которые как правило ориентируются на сектор финансовых услуг и постоянно наращивают и количество и разнообразие своих атак;

– зарубежные государственные структуры, которые интересуются кражей данных, в том числе интеллектуальной собственности из компаний-разработчиков, правительственных агентств и корпораций – военных подрядчиков;

– террористические группы, ищущие новые способы повлиять на политику США с помощью масштабных кибератак на критически важные объекты инфраструктуры, от которых в очень существенной степени зависит весь американский образ жизни.

Именно это, по нашему мнению, с одной стороны, определило характер современной «внешней политики» США в киберпространстве, а с другой – обусловило новые серьёзные проблемы международной безопасности и глобальной стабильности.

Список литературы

1. *Рогов С.М.* Стратегия национальной безопасности администрации Обамы: американское лидерство в многополярном мире // Независимое военное обозрение. 11.06.2010.

2. *Роговский Е.А.* Глобальные информационные технологии – фактор международной безопасности // США ❖ Канада. 2010. № 12. С. 3–26.

3. *Роговский Е.А.*, *Шариков П.А.* Контроль над Интернетом и международная стабильность // США ❖ Канада. 2007. № 3. С. 93–110.

4. 2010 Quadrennial Defense Review (http://www.defense.gov/qdr/qdr%20as%20of%2029jan10%201600.PDF).

5. Blueprint for a Secure Cyber Future. The Cybersecurity Strategy for the Homeland Security Enterprise. November 2011 (http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf).

6. *Clinton H.R.* Internet Rights and Wrongs: Choices & Challenges in a Networked World. George Washington University Washington, DC. 15.02.2011.

7. *Clinton H.R.* Remarks on Internet Freedom Secretary of State // The Newseum. Washington, DC. 21.01.2010.

8. Condoleeza's Letter on Internet Governance (http://www.theregister.co.uk/2005/12/02/rice_eu_letter/print.html).

9. Congress Sanctions Offensive Military Action in Cyberspace. 15.12.2011 (https://www.infosecisland.com/blogview/18769-Congress-Sanctions-Offensive-Military-Action-in-Cyberspace.html).

10. Department of Defense Cyberspace Policy Report to Congress. November 2011 (http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf).

11. Department of Defense Strategy for Operating in Cyberspace (http://www.defense.gov/news/d20110714cyber.pdf).

12. Foreign Economic Collection Report 2011 (http://www.globalsecurity.org/intell/library/reports/2011/foreign-economic-collection_2011.pdf).

13. GAO-10-606 United States Faces Challenges in Addressing Global Cybersecurity and Governance (http://www.gao.gov/new.items/d10606.pdf).

14. *Hathaway M.E.* Strategic Advantage: Why America Should Care about Cybersecurity. Harvard Kennedy School. October 2009 (http://belfercenter.ksg.harvard.edu/files/Hathaway.Strategic%20Advantage.Why%20America%20Should%20Care%20About%20Cybersecurity.pdf).

15. International Strategy for Cyberspace Prosperity, Security, and Openness in a Networked World. May 2011 (http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf).

16. *Lynn W.J., III.* Defending a New Domain: The Pentagon's Cyberstrategy // Foreign Affairs. September-October 2010 (www.foreignaffairs.com/articles/66552/william…/defending-a-new-domain).

17. *Lynn III W.J.* The Pentagon's Cyberstrategy, One Year Later. Defending against the Next Cyberattack // Foreign Affairs. September-October 2011 (http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later).

18. *McConnell M.* On How to Win the Cyber-war We're Loosing // The Washington Post. 28.02.2010 (http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493_pf.html).

19. Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers (http://www.icann.org/en/about/agreements/mou-jpa/icann-mou-25nov98-en.htm).

20. *Miles D.* Doctrine to Establish Rules of Engagement against Cyber Attacks. October 2011 (http://www.defense.gov/news/newsarticle.aspx?id=65739).

21. National Security Strategy (2010) (http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf).

22. National Defense Authorization Act for Fiscal Year 2012. Conference Report H.R. 1540. 12.12.2011 (http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt329/pdf/CRPT-112hrpt329-pt1.pdf).

23. Obama's Speech to the United Nations General Assembly. 23.09.2009 (http://www.bydewey.com/obamaun.html).

24. *Slaughter A.-M.* A New World Order. Princeton University Press. 2005. 368 p.

25. *Stiglitz J.E.* The Future of Global Governance // Initiative for Policy Dialogue (IPD). IPD Working Paper. 2004.

26. *Stiglitz J.E.* Global Public Goods and Global Finance: Does Global Governance Ensure that the Global Public Interest Is Served? // Advancing Public Goods / Ed. by J.-Ph. Touffut. Paris: Cournot Centre for Economic Studies, 2006. P. 149-164.

27. Sustaining U.S. Global Leadership: Priorities for 21th Century Defense. DoD. January 2012 (http://www.defense.gov/news/Defense_Strategic_Guidance.pdf).

28. The Comprehensive National Cybersecurity Initiative (http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative).

29. www.fbi.gov/news/stories/2012/march/shawn-henry_032712