IV. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 327

© Карасев П.А
Karasev P.

ЭВОЛЮЦИЯ ВЗГЛЯДОВ И ПОДХОДОВ США К ИСПОЛЬЗОВАНИЮ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ВОЕННО-ПОЛИТИЧЕСКИХ ЦЕЛЯХ

THE EVOLUTION OF VIEWS AND APPROACHES OF THE USA TOWARDS MILITARY-POLITICAL USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Аннотация. *Статья посвящена тому, как изменился подход США к использованию информационно-коммуникационных технологий в военно-политических целях за последние десять лет. Акцент сделан на создании нового поля военно-политического противоборства. Использование информационно-коммуникационных технологий в военно-политических целях оказывает значительное влияние на развитие военной мысли и международную безопасность. Сделан вывод о необходимости противодействовать новым угрозам, исходящим из киберпространства, при этом сохранив его позитивный потенциал.*

Annotation. *The article focuses on the shift of approach in the USA over the last ten years towards military application of ICTs. An analysis touches upon the creation of a new field of military-political confrontation. The use of information and communication technologies for military-political purposes has a significant impact on military thought and international security. It is concluded, that we need to counter new threats emanating from cyberspace, while retaining its positive potential.*

Ключевые слова. *Информационная безопасность, кибербезопасность, США, Россия, национальная безопасность, внешняя политика, вредоносное программное обеспечение, «кибероружие», Интернет.*

Key words. *Information security, cybersecurity, the USA, Russia, foreign policy, national security, malicious software, "cyberweapons", the Internet..*

Введение

Развитый мир находится под мощным влиянием информационно-коммуникационных технологий (ИКТ). Национальные информационные инфраструктуры сегодня являются одной из основ экономического, оборонного и политического потенциала государств. Возрастающая зависимость от ИКТ провоцирует использование уязвимостей компонентов информационных инфраструктур для реализации различных угроз, проявляющихся в информационном пространстве. Международным сообществом признаётся существование трёх разновидностей таких угроз, различающихся ожидаемым эффектом: использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях, в террористических целях и в военно-политических целях. [3]

Использование ИКТ в качестве средства силового воздействия оказывает значительное влияние на развитие военной мысли. В начале XXI века появилась принципиальная возможность воздействия на физический мир через виртуальную среду и произошла эволюция как взглядов политического руководства различных государств на возможность политического и военно-стратегического противостояния в информационном и киберпространстве, так и понимания, как можно использовать ИКТ не в качестве дополняющего (обеспечивающего) элемента противоборства, а как самостоятельный инструмент в этой деятельности. Первой страной, которая выработала подходы такого использования, стали США. В статье рассмотрены этапы эволюции взглядов и

Карасев Павел Александрович – научный сотрудник, Институт проблем информационной безопасности МГУ имени М.В. Ломоносова, тел. 8(495)932-89-58.

Karasev Pavel – researcher, Institute of information security issues, Lomonosov Moscow state university, tel. 8(495)932-89-58.

подходов к использованию ИКТ ВС США, вплоть до того момента, когда киберпространство было признано театром военных действий и было создано Киберкомандование США, а также проведен анализ того, как использование ИКТ в военно-политических целях оказывает влияние на международную безопасность.

Предпосылки и современное состояние взглядов и подходов США к использованию ИКТ в военно-политических целях

Анализ документов военного планирования США показывает, что отправной точкой современного состояния (когда зависимость вооруженных сил США от ИКТ создаёт проблему кибербезопасности, и в то же время обладание специализированными ИКТ делает возможным проведение наступательных кибероперaций) является внедрение в военное строительство США доктрины сетецентрических войн.

Эта доктрина была представлена в «Концепции развития вооруженных сил США до 2010 года» [9], вышедшей в 1996 г., принята в «Четырёхлетнем прогнозе Министерства обороны» 1997 г. и впоследствии развита в «Концепции развития вооруженных сил США до 2020 года» [10], вышедшей в 2000 году. В этих документах рассмотрены возможности внедрения доктрины сетецентричных войн с учетом развития ИКТ, а также особенности достижения информационного превосходства[1] с использованием ИКТ [9]. Принятие доктрины сетецентрических войн было продиктовано стремлением повысить возможности участников боевых действий за счет их объединения в единую сеть и достижения информационного превосходства.

Для обеспечения самой возможности проведения сетецентричных операций была создана соответствующая информационная инфраструктура и так называемый «информационный грид» – единая информационная система, к которой подключены и имеют доступ все боевые единицы, задействованные на театре военных действий (ТВД). При этом стала очевидной необходимость обеспечения безопасности элементов информационной инфраструктуры от внешних воздействий, которые представляют собой как физическое уничтожение технических средств передачи данных, так и внесение искажений в информационные тракты, постановку «сетевых помех», препятствующих приему информации и т.п. В «Концепции развития вооруженных сил США до 2020 года» было отмечено, что операции в информационном пространстве в перспективе станут отдельным видом вооруженной борьбы и приобретут такое же значение, как операции в других средах – на воде, суше, в воздухе и космосе. В этом документе также отмечено, что США должны стремиться к доминированию во всех этих средах, в том числе и в киберпространстве. Все дальнейшие действия США по развитию возможностей ведения наступательных и оборонительных действий в киберпространстве – *это шаги к достижению доминирования в киберпространстве.*

Ключевые изменения во взглядах и подходах США к использованию ИКТ в военно-политических целях произошли в первом десятилетии XXI века. В 2001 г. в обновленной «Четырехлетней программе развития обороны США» [18] операции, осуществляемые в киберпространстве, были выделены в самостоятельный вид деятельности, и киберпространство было признано новой сферой противоборства, наряду с сушей, водным, воздушным и космическим пространством. Как указано в этом документе, Министерство обороны США рассматривает информационные операции, разведку и силы и средства в космосе уже не просто как дополнение к существующим силам, а как ключевые возможности ВС будущего. В то же время было сказано, что деятельность ВС в киберпространстве носит оборонительный характер [18]. Чтобы обеспечить возможность вести *наступательные действия и активную оборону* в киберпространстве, в феврале 2003 года Администрация Президента Дж. Буша объявила о планах разработать уставной документ по ведению операций в киберпространстве.

В рамках разработки уставного документа происходил анализ и закрепление основных характеристик киберпространства с точки зрения потенциала военно-политического использования ИКТ. В «Национальной военной стратегии США» 2004 г. выделены следующие аспекты киберпространства[16]:

- создаётся, поддерживается, принадлежит и управляется общественными организациями, частным сектором и государствами и существует во всем мире;
- проникает через общепринятые организационные и геополитические границы;
- может использоваться другими государствами, организациями, партнёрами, частным сектором и противниками США.

С учетом этих аспектов, в «Национальной военной стратегии США» было выделено пять направлений дея-

[1]Информационное превосходство определяется в «Концепции» как способность собирать, обрабатывать и распространять непрерывный поток информации, при этом препятствуя осуществлению подобных действий противником.

тельности вооруженных сил США в киберпространстве, которые в дальнейшем получили отражение в разработанном уставном документе:

• обеспечение законного и санкционированного доступа к информации, в то же время предотвращение несанкционированного доступа и раскрытия информации (сетевые операции);

• *информационные операции воздействия на заданные аудитории для поддержания политики и интересов правительства США*;

• физическое воздействие на сети и системы;

• правоохранительные действия;

• контрразведка.

Уставный документ по осуществлению оборонительных и наступательных действий в киберпространстве появился в 2006 г. под названием «Национальная военная стратегия для операций в киберпространстве». В этом документе регламентированы все основные аспекты оборонительных и наступательных действий ВС США в киберпространстве. Дана общая характеристика киберпространства, а также выделены основные направления деятельности Министерства обороны США в этой сфере, в том числе аспекты повседневного функционирования, осуществления военных и разведывательных операций. Согласно «Четырёхлетнему прогнозу Министерства обороны» 2006 года, основной целью деятельности в киберпространстве стало сдерживание (deterrence) противников от создания и применения наступательных средств против интересов США в киберпространстве. При этом, как указано в «Национальной военной стратегии для операций в киберпространстве», деятельность в киберпространстве осуществляется при взаимодополняющем использовании наступательных и оборонительных операций, в том числе за пределами государственных границ. Важно также отметить, что речь идёт не только о кибероперациях, но и операциях в информационном пространстве, поскольку «Интернет и компьютерные сети являются одним из способов воздействия Министерства обороны на зарубежную аудиторию в государственных интересах США в рамках комплекса мероприятий, предпринимаемых ведомствами США».

«Всеобъемлющая инициатива национальной кибербезопасности»[6] и «Национальная стратегия обороны США»[13], вышедшие в 2009 и 2008 гг. соответственно, являются очередным шагом эволюции подходов к деятельности ВС США в киберпространстве. В этих документах впервые появляется тезис, что особенности киберпространства (его основу составляет инфраструктура, находящаяся в частных руках; в нем активно существует множество акторов, в том числе террористов и преступников; киберпространство трансгранично и анонимно) приводят к тому, что государство в одиночку не может обеспечить безопасность этой среды. В этой связи «Всеобъемлющая инициатива национальной кибербезопасности» «направлена на создание такой стратегии кибероборонs, которая будет основываться на сдерживании атак и проникновений через киберпространство путём развития систем предупреждения, *повышения роли частного сектора и международного сотрудничества*, а также разработки приемлемых ответов на действия государственных и негосударственных акторов» [6]. В «Национальной стратегии обороны США» этот тезис повторяется: «Министерство обороны в долгосрочной перспективе не сможет в одиночку обеспечить безопасность киберпространства. При сохранении ключевой роли Министерства обороны этим должны заниматься другие ведомства, частный сектор и партнеры на международной арене» [13]. В связи с тем, что кибершпионаж и киберпреступность наносят значительный урон национальной безопасности и экономике США, в «Стратегии» поставлена задача «определить, какие враждебные действия в киберпространстве, не ведущие к людским потерям, считать нападением на государство и на какие из них в ответ может потребоваться применение силы».

С приходом Барака Обамы на президентский пост политика США в области кибероборонs сильно изменилась, но использование ИКТ в военно-политических целях осталось и даже развилось. Принятие ряда документов и изменения в структуре ВС США перевели деятельность военных в киберпространстве на новый уровень. В дополнение к «Национальной военной стратегии операций в киберпространстве» [15] 2006 г., в 2011 г. были приняты «Национальная военная стратегия США»[14], и «Стратегия Министерства обороны США по операциям в киберпространстве» [8].

Важнейшим шагом развития способности США осуществлять наступательные и оборонительные операции в киберпространстве стало создание в 2010 г. Киберкомандования в составе Стратегического командования ВС США. В круг решаемых им задач входят: проведение операций в киберпространстве, защита военных систем и сетей, и координация взаимодействия по кибероборонe между всеми родами войск. Соответственно, все прежние тезисы о том, что киберпространство является таким же театром военных действий, как и другие среды, получили практическую реализацию. При этом глава новой структуры также является руководителем Агентства национальной безопасности США, основной функцией ко-

торого является радиоэлектронная разведка. Подчинение этих двух структур одному руководителю и заключение в 2010 г. «Меморандума о взаимопонимании»[11] между Министерством обороны и Министерством внутренней безопасности способствовало скорейшему развитию потенциала Киберкомандования по осуществлению наступательных и оборонительных действий в киберпространстве. Таким образом, кибероружие[1] стало или в перспективе должно стать полноценным наступательным инструментом в руках военных.

Взгляды на проведение операций в киберпространстве получили развитие в «Стратегии Министерства обороны США по операциям в киберпространстве» [8], вышедшей в 2011 г. Во-первых, была признана устоявшаяся в международной практике триада угроз, исходящих из киберпространства. Во-вторых, подчеркнута необходимость международного сотрудничества для защиты общих интересов и обеспечения безопасности, конкретными проявлениями которой являются коллективная самооборона и установление международных норм для киберпространства. Наконец, был раскрыт тезис о необходимости расширения всестороннего сотрудничества внутри государства, который красной нитью проходит через новое видение обеспечения кибербезопасности: для реализации комплексной программы кибербезопасности, охватывающей все правительственные учреждения, необходимо сотрудничество с другими министерствами правительства США, агентствами и частным сектором; использовать общественный потенциал для развития новых технологий и подготовки квалифицированных кадров.

Потенциал бизнеса и гражданского общества для проведения кибероперации уже активно используется. В начале 2012 г. ВВС США объявили открытый тендер на разработку комплекса специальных программных средств (то есть вредоносных программ), которые смогут решать ряд задач [5], в том числе резидентное нахождение на компьютере предполагаемого противника, слежение за активностью информационных систем противника, выведение их из строя. Однако ещё в 2011 году, отвечая на вопросы конгрессменов, представитель Министерства обороны США подтвердил наличие у Америки наступательного кибероружия [7].

Кроме активного рекрутинга хакеров [22], Министерство обороны США в лице своего Агентства передовых разработок (DARPA) приступило к разработке проекта под названием «Project X» [25]. Он направлен на создание такого программно-аппаратного комплекса, который даст возможность применять кибероружие простым военнослужащим, не имеющим специального образования, и упростит запуск вредоносной программы. При этом будет создан единый аппаратно-программный комплекс и интерфейс пользователя, который объединит множество вредоносных программ, разрабатываемых вне Министерства обороны – сторонними подрядчиками. Конечному пользователю останется лишь выбрать цель, средства поражения и нажать на пуск – всё остальное автоматизировано.

Очевидно, что выстраивается определенная иерархия, в которой будет несколько видов кибероружия. Одно будет применяться для решения тактических задач без специального согласования и ограничено по месту и времени действия – для поражения компьютерных сетей и систем противника на ТВД. Другое стратегическое, более сложное будет предназначено для выведения из строя критически важных объектов потенциального противника, будет санкционировано к применению на более высоком уровне в рамках проведения специальных операций. Кроме наступательных возможностей, развиваются элементы оборонительных систем. Во «Всеобщей инициативе национальной кибербезопасности» 2008 г. упомянуты проекты EISTEIN. Формально эти программы предназначены для обороны и работают методом анализа и фильтрации Интернет-трафика. Однако на следующем этапе их развития, помимо этапа проверки, предполагается автоматическое противодействие угрозам вторжения, что представляет собой систему активной обороны.

Деятельность в киберпространстве находится в числе главных приоритетов Министерства обороны США, о чем свидетельствуют и объёмы финансирования. В документе «Поддержание лидерства США – приоритеты развития обороны в XXI веке», вышедшем в январе 2012 г., расставлены приоритеты в ситуации сокращения расходов – и одним из направлений, по которым планируется рост финансирования, а не его сокращение, являются действия в киберпространстве. В оборонном бюджете на 2014 г. (Закон о национальной обороне [12]), принятом Конгрессом США, количество слов с частью «кибер», по сравнению с аналогичным документом 2012 г., возросло более чем в 10 раз – с 12 до 127. На развитие деятельности Министерства обороны в кибер-

[1]В настоящее время идут активные дискуссии среди специалистов, что понимать под термином «кибероружие». В настоящей статье используется выработанное в ходе реализации совместного проекта Института проблем информационной безопасности МГУ и Института «Восток-Запад» (США) определение: программное, аппаратное обеспечение, или прошивки микросхем, разработанные и/или применяемые для нанесения ущерба в киберсфере см. URL: http://iisi.msu.ru/articles/article31/.

пространстве в 2014 г. будут затрачены миллионы долларов, которые пойдут, в частности, на создание специальных киберполигонов для подготовки специалистов, анализ кибероперациий в целом, разработку специальных средств и создание поста главного советника по кибероборонe, в задачи которого будет входить руководство обороной США от угроз, исходящих из киберпространства. 68 млн. долл. направлено на поддержание функционирования Киберкомандования. 19 млн. долларов – на кибер программы ВВС США, в том числе 5,8 млн. на оборонительные и 14 млн. (в 2,5 раза больше!) на наступательные. Из 40 млн. долл., выделенных на финансирование исследований в области кибербезопасности, поровну разделено между текущими и перспективными исследованиями.

На фоне растущих затрат на разработку кибероружия возрастает активность США по продвижению своих интересов в вопросах кибербезопасности на международном уровне.

На саммите НАТО в Лиссабоне в 2010 г. США удалось включить кибербезопасность в число приоритетных задач [17] и начать выработку соглашений по кибероборонe. Генеральный секретарь НАТО Расмуссен подчеркнул, что «Североатлантический альянс должен быть готов к новым вызовам, среди которых атаки в киберпространстве» [24]. Важным стало заявление Госсекретаря США Хиллари Клинтон во время её выступления на заседании Атлантического совета в феврале 2010 г.: «Такие угрозы компьютерным сетям и инфраструктуре НАТО, как кибератаки, должны быть рассмотрены с точки зрения 5-й статьи Североатлантического договора» [21].

В августе 2012 г. Таллиннским центром кибероборонe НАТО было представлено «Таллиннское руководство по применимости международного законодательства к кибервойнам» [19]. Этот документ, хотя и не несёт никакой юридической силы для международного сообщества, очень важен, поскольку представляет собой согласованное мнение экспертов государств-участников блока НАТО по проблеме кибервойн и киберконфликтов. Принципы адаптации существующих норм международного права к киберконфликтам, заложенные в «Таллинском руководстве» приведут к необходимости согласования заново всего массива международного гуманитарного права.

В оборонном бюджете США на 2014 г. есть пункт о запуске «Инициативы кибербезопасности»[12], суть которой заключается в попытке установления контроля над распространением кибероружия, а причина – рост угрозы от таких «кибербомб», как STUXNET и создание специальных киберподразделений в зарубежных государствах. Итогом межведомственного процесса по выработке и продвижению этой инициативы должно стать пресечение торговли кибероружием и соответствующей инфраструктурой, которые могут быть использованы в преступных, террористических и военных целях, но при этом государства должны быть способны использовать эти инструменты для законной самообороны. Таким образом, возможно, что в ближайшее время США предложат новую национальную стратегию или международный документ, который будет регулировать оборот кибероружия. Учитывая, что кибероружие имеет форму компьютерных программ, ограничить его распространение будет практически невозможно – так же, как невозможно полностью пресечь распространение нелицензированных копий других программ и мультимедийного контента. Следовательно, такой документ, если он появится, будет носить политический характер и будет направлен на ограничение круга акторов, допущенных к оборонительным и наступательным возможностям в киберпространстве. При сохранении лидерства США в этой сфере такой документ будет направлен, в том числе и на ограничение возможностей государств, которые не обладают возможностями разработки собственных средств кибероборонe.

Как уже было сказано, с приходом Б.Обамы на пост Президента одним из направлений развития системы кибербезопасности США стало международное сотрудничество. После многих лет неучастия, а порой и противодействия инициативам России в области международной информационной безопасности сегодня американская сторона принимает активное участие в работе Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Также существенно расширилось конструктивное взаимодействие с Россией по некоторым вопросам кибербезопасности. Летом 2013 года было подписано «Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия»[2]. Помимо важных пунктов об укреплении мер доверия и развитии двусторонней работы, внимания заслуживает то, что в заявлении говорится, что эти меры могут содействовать дальнейшему продвижению норм мирного и законного поведения в отношении использования ИКТ на межгосударственном уровне. Фактически США признали существование угрозы военно-политического использования ИКТ и необходимости борьбы с ней. Это может свидетельствовать и о том, что США достигли определенного уровня доминирования в киберпространстве и диалог о регулировании

этой сферы не повредит их интересам, а напротив, ограничив круг участников, закрепит статус-кво.

Выводы

Угрозы, исходящие из информационного пространства, в том числе использование ИКТ в военно-политических целях, за последние несколько лет стали мощным дестабилизирующим фактором международных отношений. В рассмотренный в настоящей статье временной период США последовательно осуществили ряд взаимосвязанных политических и организационных шагов по развитию своих возможностей ведения оборонительных и наступательных операций в киберпространстве:

1. США доктринально закрепили за киберпространством статус пятого театра военных действий (наряду с сушей, водой, воздухом и космосом).

2. Был разработан и утвержден целый ряд документов, в том числе уставного характера, в которых были обоснованы и закреплены основы проведения оборонительных и наступательных операций в киберпространстве.

3. Для осуществления наступательных и оборонительных операций в киберпространстве была создана управляющая структура и специальные подразделения, в которые активно привлекаются талантливые хакеры.

4. Кибербезопасность была включена в число приоритетных направлений стратегического развития НАТО[17] и действие 5-й статьи Североатлантического договора фактически было расширено на нападения из киберпространства[23]. При этом у экспертов и политиков как российских, так и западных есть понимание, что на современном этапе развития ИКТ невозможно точно определить источник нападения из киберпространства. Это означает, что в случае применения 5-й статьи виновный будет назначен.

5. Признавая, что ни одно государство не может обеспечить кибербезопасность в одиночку, США в последнее время активно сотрудничают по некоторым вопросам кибербезопасности с другими странами, в том числе поддерживают отдельные инициативы России и участвуют в работе Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

Анализ динамики развития возможностей США по использованию ИКТ в военно-политических целях позволяет выделить следующие направления этого развития на ближайшую перспективу:

1. Международное сообщество в докладе Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности признало использование ИКТ в военно-политических целях угрозой международному миру и безопасности. Несмотря на это развитие оборонительных и наступательных возможностей в киберпространстве для США остается приоритетным направлением и продолжится стремительными темпами с привлечением ресурсов бизнеса и даже гражданского общества. Также продолжится развитие систем кибероборонны НАТО.

2. США продолжат создание наиболее отвечающего своим национальным интересам (обеспечить доминирование в киберпространстве) правового режима для кибероружия: продолжится работа по адаптации международного гуманитарного права и права ведения войны; будет предпринята попытка ограничить торговлю кибероружием, возможно, в рамках расширения списков Вассенарских соглашений[20].

В условиях не прекращающейся милитаризации киберпространства для противодействия угрозе использования ИКТ в целях, оказывающих негативное воздействие на международный мир и безопасность, необходимо:

• обеспечить практическую реализацию принятых решений, направленных на создание национальной системы обеспечения информационной безопасности и киберкомандования в структуре Вооруженных сил Российской Федерации[4];

• продолжить активную деятельность по продвижению инициатив в области международной информационной безопасности на международной арене в многостороннем и двустороннем формате, в особенности с США и КНР, по реализации задач, поставленных в «Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года»[1], среди которых – «регламентация применения принципов и норм международного гуманитарного права в сфере использования ИКТ» и «создание условий для установления международного правового режима нераспространения информационного оружия».

Литература

1. «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года», утверждены Президентом Российской Федерации В.Путиным 24 июля 2013 г., № Пр-1753. // Совет Безопасности Российской Федерации [Официальный сайт] URL: http://www.scrf.gov.ru/documents/6/114.html.

2. Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия // Президент России [Официальный сайт] URL: http://www.kremlin.ru/ref_notes/1479.
3. Резолюция ГА ООН 54/49 Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности // ООН. [Официальный сайт]. URL: http://daccess-ods.un.org/access.nsf/Get?Open&DS≠A/RES/54/49&Lang≠R.
4. Шойгу вернулся к идее Рогозина создать киберкомандование. Алексей Михайлов, Дмитрий Бальбуров // Известия [Электронный ресурс] URL: http://izvestia.ru/news/544703.
5. Broad Agency Announcement – Cyberspace Warfare Operations Capabilities // Federal Business Opportunities [Официальный сайт] URL: https://www.fbo.gov/utils/view?id≠48a4eeb344432c3c87df0594068dc0.
6. The Comprehensive National Cybersecurity Initiative // The White House [Официальный сайт] URL: http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf.
7. Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 // US Department of Defense. [Официальный сайт] URL: http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf.
8. Department of Defense Strategy for Operating in Cyberspace // US Department of Defence. [Официальный сайт]. URL: http://www.defense.gov/news/d20110714cyber.pdf.
9. Joint Vision 2010 // The Defense Technical Information Center. [Официальный сайт]. URL: http://www.dtic.mil/jv2010/jv2010.pdf (дата обращения: 1.02.2014).
10. Joint Vision 2020 // US Forest Service. [Официальный сайт]. URL: http://www.fs.fed.us/fire/doctrine/genesis_and_evolution/source_materials/joint_vision_2020.pdf.
11. Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity // US Department of Homeland Security. [Официальный сайт] URL:http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf .
12. National Defense Authorization Act for Fiscal Year 2014 // The Library of Congress. [Официальный сайт] URL:http://thomas.loc.gov/cgi-bin/query/z?c113:H.R.3304:.
13. National Defense Strategy, 2008// US Department of Defense. [Официальный сайт] URL: http://www.defense.gov/news/2008%20national%20defense%20strategy.pdf.
14. The National Military Strategy, 2011 // US Army. [Официальный сайт] URL:http://www.army.mil/info/references/docs/NMS%20FEB%202011.pdf.
15. The National Military Strategy for Cyberspace Operations, 2006 // US Department of Defense. [Официальный сайт]. URL: http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf.
16. The National Military Strategy of the United States of America – A Strategy for Today, a Vision for Tomorrow, 2004 // US Department of Defense. [Официальный сайт]. URL: http://www.defense.gov/news/Mar2005/d20050318nms.pdf .
17. NATO new Strategic Concept // NATO [Официальный сайт]. URL:http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf.
18. Quadrennial Defense Review 2001 // US Department of Defense. [Официальный сайт]. URL:http://http://www.defense.gov/pubs/qdr2001.pdf.
19. Tallinn manual on the international law applicable to cyber warfare // NATO cooperative cyber defense centre of Excellence. [Официальный сайт] URL: http://www.csef.ru/files/csef/articles/3990/3990.pdf.
20. Cyber war technology to be controlled in same way as arms. Sam Jones // Financial Times [Электронный ресурс] URL: http://www.ft.com/intl/cms/s/0/2903d504-5c18-11e3-931e-00144feabdc0.html≠axzz2t654Wg58 (дата обращения: 1.02.2014).
21. Joyner J. Clinton: Cyber Security and Energy Security as NATO Priorities. New Atlanticist: Policy and AnalysisBlog, February 23, 2010 // Atlantic Council. [Официальный сайт]. URL: http://www.acus.org/new_atlanticist/clinton-cyber-security-and-energy-security-nato-priorities .
22. Kopstein J. NSA trolls for talent at DefCon, the nation's largest hacker conference// The Verge [Электронный ресурс] URL:http://www.theverge.com/2012/8/1/3199153/nsa-recruitment-controversy-defcon-hacker-conference .
23. Smith M., Warren P. NATO warns of strike against cyber attackers // The Sunday Times June 6, 2010.
24. Busse N., Rasmussen: In der Nato muss sich viel ändern // Frankfurter Allgemeine, October 11, 2010.
25. This Pentagon Project Makes Cyberwar as Easy as Angry Birds // WIRED [Интернет-ресурс] URL: http://www.wired.com/dangerroom/2013/05/pentagon-cyberwar-angry-birds/all/.

Материал поступил в редакцию 25. 02. 2014 г.