УДК 32+33(73)

ПЕНТАГОН УСИЛИВАЕТ КИБЕРОБОРОНУ

© 2011 г. **Е.А. Роговский, П.А. Шариков***
Институт США и Канады РАН, Москва

Авторы анализируют основные тезисы статьи Уильяма Дж. Линна, посвящённой направлениям политики Министерства обороны по защите интересов США в информационном пространстве и приходят к заключению, что в США началась новая технологическая эра.

Ключевые слова: *Информационная безопасность, киберкомандование, информационные технологии, национальная безопасность, Пентагон.*

Начало технологической эры

В статье заместителя министра обороны США У.Дж. Линна «Защищая новое пространство: стратегия кибербезопасности Пентагона», опубликованной в осенней книжке журнала «Форин афферс» [4], утверждается, что в XXI веке США вступают в новую технологическую эру – эру кибербезопасности. Эта работа заместителя министра обороны США, безусловно, будет иметь большое теоретическое значение, причём не только для сферы военно-политических исследований, но также и для экономической науки, изучающей общие тенденции и периодизацию этапов («эр», «эпох», «укладов») технологического развития общества.

Как нам представляется, У. Линн оказался одним из первых, кто пришёл к выводу, что именно технологии обеспечения безопасности информационного пространства уже стали и останутся в долгосрочной перспективе ведущими, если не доминирующими. Его позицию можно понять так, что происходящая в настоящее время технологическая революция в США ориентируется на преодоление *очень существенных негативных* последствий нынешнего информационно-коммуникационного «уклада».

Для российского читателя, воспитанного на широко известных трудах академиков Д.С. Львова и С.Ю. Глазьева и их последователей, это звучит, по крайней мере, странно. В самом деле, у нас принято считать, что процесс технологического совершенствования в целом носит рациональный (позитивный) характер и что этот процесс обусловлен исключительно *повышением эффективности общественного производства.*

* **РОГОВСКИЙ Евгений Александрович – кандидат экономических наук, руководитель Центра военно-промышленных проблем ИСКРАН**. E-mail: Rogowsky@mail.ru; **ШАРИКОВ Павел Александрович – кандидат политических наук, научный сотрудник Центра**. E-mail: pasha.sharikov@gmail.com

Как считает академик С.Ю. Глазьев, «с середины 1980-х годов повышение эффективности общественного *производства* развитых стран мира связывается с широким распространением так называемого пятого технологического уклада (информационных и коммуникационных технологий), опирающегося на два ключевых фактора 1) микроэлектронику и 2) программное обеспечение. Сегодня этот технологический уклад близок к пределам своего роста: взлёт и падение цен на энергоносители, образование и крах финансовых пузырей – верные признаки завершающей фазы жизненного цикла доминирующего в настоящее время технологического уклада и начала структурной перестройки экономики на основе следующего – *шестого технологического уклада*[*], становление и рост которого будут определять глобальное развитие в ближайшие два-три десятилетия. Граница между пятым и шестым укладами лежит в глубине проникновения технологии в структуры материи и масштабах обработки информации» [1]. В рамках такой теории периодизации и смены технологических укладов проблемы безопасности не рассматриваются. Именно по этой причине и необходимо проанализировать позицию У. Линна.

По его мнению, начало новой технологической эпохи ознаменовано ошеломляющей серией кибератак, которым подвергаются американские Интернет-ресурсы последние десять лет – каждый день на военные и гражданские сети США обрушиваются тысячи кибератак, в том числе направленных на американские военные сети, причём частота и изощренность последних быстро возрастает. Так, в конце 2008 г. Министерство обороны США подверглось кибератаке, и военные компьютерные сети были поражены «киберчервём», который, по мнению Пентагона, был запущен иностранной спецслужбой. Атака стала следствием того, что заражённая вирусом флэшка была вставлена в один из интегрированных в сеть МО компьютеров, находящихся на военной базе США на Ближнем Востоке. В результате этот вирус незаметно распространился по компьютерной сети Центрального командования и заразил секретные и несекретные информационные системы. Вредоносная программа создала брешь, через которую неизвестный противник получил доступ к тысячам файлов из закрытых сетей США (а также их союзников и бизнес-партнёров), в том числе к проектам создания новых систем вооружения, планам проведения операций, данным разведки.

И эта атака, как утверждает Линн, не была единственной. По сообщениям прессы, в апреле 2009 г., хакерами был взломан особый банк данных и украдена технологическая документация по новому американскому истребителю «Лайтнинг-III» (*F-35 Lightning III*) [3]. Обобщая имеющиеся данные о такого рода инцидентах, бывший руководитель Агентства национальной безопасности США и директор Национальной разведки США адмирал М. МакКоннелл неоднократно предупреждал, что в отношении военных информационных ресурсов вопросы кибербезопасности стоят в США особенно остро. В статье, недавно опубликованной в газете «Вашингтон пост», он высказался достаточно жестко: «США уже находятся в состоянии информационной войны и проигрывают её» [5].

[*] Шестой уклад характеризуется использованием нанотехнологий и биокомпьютеров, на этом уровне появляется возможность менять молекулярную структуру вещества, придавать ему принципиально новые свойства, видоизменять клеточную структуру живых организмов.

Бывший руководитель Национальной разведки Д. Блэр также не раз обращал внимание на возрастающее количество кибератак (как он утверждал, особенно со стороны Китая и России). У. Линн отмечает, что наступательный потенциал для операций в киберпространстве развивают многие противодействующие США страны; около 100 организаций и иностранных разведок стремятся внедриться в американские сети, а некоторые из них уже имеют возможность частично разрушить американскую информационную инфраструктуру.

Однако официально считать кибератаки актом агрессии и предпринимать против агрессора ответные меры, как оказалось, очень не просто. Но и игнорировать складывающуюся ситуацию военные просто не имеют права.

Здесь главное состоит в том, чтобы понять, что именно происходит, чтобы адекватно осознать происходящую трансформацию, а также связанные с нею угрозы. В этом контексте У. Линн напоминает о широко известном письме, написанном в начале августа 1939 г. и адресованном Франклину Рузвельту. В нем знаменитый физик А. Эйнштейн сообщал президенту США о том, что научные результаты, полученные в области ядерного синтеза, достаточно быстро могут привести к созданию атомной бомбы. Фактически А. Эйнштейн предупредил о скором начале новой технологической трансформации, что и подвигло Рузвельта запустить «Манхэттенский проект», который, как считает заместитель главы Пентагона, своевременно подготовил Соединённые Штаты к наступлению ядерной эры.

По его мнению, кибератаки подобны ядерному оружию в том отношении, что они предоставляют одной из противоборствующих сторон возможность преодолеть подавляющее превосходство другой стороны в обычных вооружениях. И хотя они, видимо, не могут привести к массовым потерям, сопоставимым с потерями от ядерного удара, кибератаки тоже могут парализовать американское общество; иначе говоря, иметь неприемлемые последствия. Так, непосредственную угрозу экономике представляют кибератаки, направленные против критически важных инфраструктурных объектов – например сетей электроснабжения, коммуникационных систем или банков, а также Интернет-сетей, координирующих снабжение и тыловое обеспечение американских вооружённых сил как на территории США, так и за рубежом.

Угрозы кибербезопасности не ограничиваются военными целями. Долгосрочную стратегическую угрозу представляет систематическое проникновение хакеров в американские образовательные и коммерческие сети, что увеличивает риск промышленного шпионажа, кражи коммерческой информации и интеллектуальной собственности и в конечном счёте подрывает глобальные (военные и гражданские) конкурентные преимущества США. Обращая внимание на это обстоятельство, У. Линн подчёркивает, что из различных информационных сетей, поддерживаемых американскими корпорациями, университетами и государственными агентствами, каждый год крадётся такое количество интеллектуальной собственности, которое по своему объёму превосходит содержание Библиотеки Конгресса США.

Следует также иметь в виду, что и программное обеспечение и компьютеры подвергаются рискам ещё до того, как они интегрируются в сеть. Вредоносные программы, включая так называемые логические бомбы, которые при-

водят к внезапным нарушениям, могут быть «зашиты» в них на стадии их разработки или производства. Так называемые скрытые «потайные двери» могут оказаться внутри компьютерных чипов и открывать противнику доступ в компьютерную сеть с удалённого рабочего места. Подобное «устройство» однажды уже было найдено среди партии компьютеров, закупленных Министерством обороны США.

Новая стратегия сдерживания

Что касается военной стратегии, она начинается с того, что Пентагон признал киберпространство новым театром военных действий. Несмотря на то что киберпространство – это сфера антропогенной деятельности, она стала столь же критически важной для проведения военных операций, как суша, море, воздух или космос. Военные должны быть готовы его защищать.

Высокопоставленный чиновник убеждает читателя в том, что Пентагон должен противостоять киберугрозам, но признает, что для защиты киберпространства типичная для времен «холодной войны» ракетно-ядерная концепция стратегического сдерживания с помощью угрозы нанесения ответного удара не применима. Та концепция предполагала возможность нанесения встречного удара сразу после идентификации врага, т.е., как только определялось, чьи именно ракеты летят к вашим целям (до их поражения). Важно то, что время, необходимое для идентификации врага и получения санкции на ответный удар, меньше времени подлёта ракет. И поскольку речь идёт о космических скоростях, этого времени (нескольких минут) явно не достаточно для каких-либо парламентских процедур; здесь решение должен принимать только один человек. Поэтому Конгресс **заранее** уполномочивает президента страны принимать решения о нанесении ответно-встречного удара по конкретному противнику. Такой документ в определённом смысле решает проблему дефицита времени и предоставляет вооружённым силам необходимую оперативность.

В случае кибератаки ситуация иная. Скорость «полёта» информации в Интернете сопоставима со скоростью света, а потому для реагирования на кибернападение времени остаётся совсем мало (здесь могут играть роль миллисекунды). За это время человек принять осмысленное решение просто не в состоянии. Реагировать должны компьютеры, заранее оснащённые соответствующими программами. Однако в этом случае остаётся нерешённой 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***, – 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. 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 организаций (бизнеса) в нейтральных странах.

Поэтому У. Линн полагает, что в противодействии кибератакам концепция ответного удара, предполагающая нанесение противнику «неприемлемого возмездия», не должна быть главным элементом стратегии сдерживания, а ***главными в этой стратегии должны стать заблаговременные усилия, способные сделать такие атаки бессмысленными, безрезультатными, неэффективными***.

На подобный принцип сдерживания ещё в 2000 г. указал министр обороны в администрации Клинтона У. Коен: «Мы должны не только быть настолько сильными, чтобы успешно отразить любое нападение, но и чтобы ни у кого и мысли не появлялось напасть на нас». Именно такой подход представляет основу новой американской политики глобального сдерживания, которое опирается на ***активную превентивную оборону*** и ***абсолютное доминирование информационного потенциала США*** (на что мы раньше уже обращали внимание) [2].

Как нам представляется, в этом случае компьютерные системы, образующие эшелоны кибероборонны тех или иных информационных сетей, должны быть подобны так называемой «активной броне», отражающей попадание снаряда с помощью встречного микровзрыва. Иначе говоря, такая «активная компьютерная броня» в ответ на кибератаку должна поразить, если не самого противника, то по крайней мере запущенный им вирус. Фактически это означает, что система кибербезопасности США (подобно ракетно-ядерному щиту) должна иметь не только оборонительный, но и наступательный характер.

Заместитель министра обороны США полагает, что таким соображениям соответствует внедряемая Пентагоном трехслойная система кибероборонны. Её первые два слоя построены на передовом опыте коммерческих структур: на соблюдении обычной компьютерной антивирусной гигиены, на применении чувствительных сенсоров, выявляющих и классифицирующих кибератаки, а также на своевременном обновлении программного и аппаратного обеспечения, восстанавливающего работоспособность подвергшейся атаке системы. Задача этих двух эшелонов кибероборонны – снизить результативность кибернападения.

Но США не могут отступить за некую виртуальную «линию Мажино», построенную из оборонительных сетевых экранов («файерволов») и смириться с большим риском того, что информационные сети могут быть в любой момент повреждены. В ситуации кибервойны строить системы пассивной обороны (крепости) может оказаться бессмысленной затеей, в такой ситуации решающее значение может приобрести скорость и маневренность ***наступательных операций***. Поэтому Пентагон создаёт третью линию обороны, которая опирается на (весь!) национальный разведывательный потенциал, и призвана обеспечить «высоко специализированную активную оборону», в частности, распознавание источника атаки («лишение противника анонимности») и его нейтрализация.

Наступательный характер активной кибероборонны Пентагона нашёл подтверждение в ряде выступлений шефа военного Киберкомандования США генерала К. Александера, который хотел бы получить полномочия на осуществление «полного спектра» операций в киберпространстве. В августе 2010 г. К. Александер заявил, что и в этой сфере «мы должны иметь наступатель-

ный потенциал, способный в реальном времени сбивать всех, кто пытается нас атаковать». Для устранения киберугроз США «должны обладать динамичной активной защитой», способной отбросить их как можно дальше от границ охраняемого периметра. Такую защиту К. Александер представил как «охоту» за вредоносными программами внутри компьютерных сетей, используемых противником. Фактически при этом речь идёт о полномочиях Пентагона на проведение наступательных операций в Интернет-пространстве, имеющих целью предотвращение направленных против США кибератак путём частичного разрушения компьютерных сетей противника или модификацию программных кодов его компьютеров (для обезвреживания имеющихся в них вредоносных программ).

Очевидно, что без тесного взаимодействия с разведкой решение этой задачи невозможно, а потому Киберкомандование США тесно сотрудничает с Агентством национальной безопасности (АНБ), осуществляющим все виды электронного перехвата иностранных целей. Интересно отметить, что штабквартира Киберкомандования США расположена в Форт-Миде на том же этаже, где расположен офис директора АНБ.

Однако многие чиновники администрации президента Обамы и авторитетные в США юристы считают необходимым ограничить наступательный киберпотенциал Пентагона только зоной военных действий, такой, например, как Афганистан. Отчасти такое ограничение обусловлено позицией ЦРУ, которое относит все операции вне зоны боевых действий к сфере своей компетенции. В свою очередь Государственный департамент озабочен тем, что отсутствие такого ограничения может иметь серьёзные дипломатические последствия. Так, операции против цели в одной стране могут непреднамеренно поразить серверы в другой стране, как это случилось в 2008 г., когда киберподразделение под К. Александера, нанесло удар по веб-сайтам исламских террористов.

Более того, учитывая кризисную финансовую ситуацию, в которой уже несколько лет находится американская экономика, администрация Обамы заставляет Пентагон экономить «по крупному», вынуждая его планировать масштабные сокращения расходов на подготовку к будущей «большой войне» и сосредоточить деньги на обеспечении текущих конфликтов малой интенсивности. Очевидно, что на этом фоне вопросы кибероружия приобретают стратегический характер, а потому Пентагон объявил, что до конца 2010 г. он подготовит и предложит президенту новую версию национальной стратегии обеспечения кибербезопасности.

Всё это и составляет основу новой стратегии, принципиально отличающейся от доктрины ядерного сдерживания, и заслуживает поэтому самого серьёзного внимания, причём не только со стороны специалистов, занятых военно-политическими исследованиями. Внимательно прочитав данную статью, читатель не может не прийти к выводу о том, что основные риски (угрозы), связанные с наступление эры кибербезопасности, Пентагон осознал и уже располагает новой стратегией, цель которой состоит в том, чтобы сделать американское киберпространство безопасной средой, а также использовать его для укрепления национальной (в том числе экономической) безопасности Соединённых Штатов.

Основу этой стратегии составляет концепция организационной структуры кибероборонь США, включающая:

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

Последние несколько лет, действия военных по обеспечению безопасности киберпространства проводились плохо скоординированными различными рабочими группами, организационно не связанными друг с другом. Для реализации изложенной стратегии кибероборонь и проведения военных операций в киберпространстве, Министерство обороны США свою организационную структуру изменило. Оно приступило к созданию надёжной многоуровневой обороны военных сетей. В июне 2009 г., признавая, что защита киберпространства значительно уступает существующим военным угрозам, министр обороны Р. Гейтс приказал объединить все рабочие группы в единое Киберкомандование высшего уровня (*U.S. Cyber Command*), которое в мае 2010 г. стало частью американского стратегического командования (STRATCOM). Именно на него возложена ответственность за интеграцию действий по обеспечению кибербезопасности военных компьютеров. Упомянутые выше кибератаки стали сигналом для активизации оборонительных действий в сфере киберпространства, а ключевым элементом в военной стратегии кибероборонь стала специальная операция Министерства обороны, известная под наименованием «Заградительная операция “Янки”» (*Operation Buckshot Yankee)*.

На Киберкомандование возложено три задачи:

1) защита всех военных сетей и поддержка военных действий и операций против кибертеррористов;

2) управление всеми военными киберресурсами и обеспечение соблюдения правил информационной безопасности во всех подразделениях Министерства обороны (Киберкомандование контролирует все ветви американкой военной киберсистемы, включающей киберкомандование американской армии, 10-й флот ВМФ, 24-ю авиабазу и киберкомандование морских пехотинцев);

3) координация и киберсотрудничество Министерства обороны с другими государственными ведомствами, союзниками и частным бизнесом.

В статье говорится, что самые лучшие планы защиты военных сетей окажутся бесполезными, если в ходе военного конфликта противник сможет вывести из строя гражданскую информационную инфраструктуру страны. В самом деле, Министерство обороны в очень существенной степени зависит от качественной работы всей информационной инфраструктуры Соединённых Штатов, в том числе гражданского Интернета. В частности, сети, работающие в гражданских доменах .gov и .com защищены существенно хуже военных доменов .mil. За безопасность первых отвечает Министерство внутренней безо-

пасности, однако Пентагон, по мнению У. Линна, также должен принимать участие в поддержке этой критически важной составляющей американской информационной инфраструктуры, хотя в настоящее время вопрос о том, как именно вооружённые силы должны участвовать в защите гражданской информационной инфраструктуры, окончательно ещё не решён. (Наиболее значимой здесь является защита промышленности, выполняющей заказы Министерства обороны.)

Учитывая глобальность Интернета, союзникам Соединённых Штатов тоже отводится очень важная роль в обеспечении кибербезопасности и прежде всего в обмене информацией об источниках кибератак. В этом контексте концепция объединённой системы предупреждения о воздушных атаках (*shared warning*), составлявшая основу прежней военной доктрины применима и к киберпространству. Иначе говоря, рекомендует У. Линн, Соединённым Штатам имеет смысл создать единую (с союзниками) систему коллективного мониторинга компьютерных сетей. При этом следует иметь в виду, что некоторые американские оборонные информационные сети уже объединены с сетями союзников, например закрытыми каналами, по которым осуществляется обмен разведывательной информацией. Здесь актуальными являются задачи повышения информационной ёмкости и оперативности.

Для повышения уровня кибербезопасности США, считает автор статьи, необходимы новые международно-правовые нормы и договоры в том числе по линии НАТО. В докладе НАТО-2020, подготовленном под руководством бывшего государственного секретаря США М. Олбрайт и посвящённом аналитической работе Североатлантического альянса, совершенно справедливо отмечается необходимость создания новой стратегической концепции альянса*, в которой интегрированы системы кибероборонны. От себя Линн добавляет, что США должны добиваться того, чтобы натовские ресурсы направлялись также и на обеспечение кибербезопасности операций альянса.

О государственных заказах

Правительство США должно противостоять угрозам кибербезопасности точно так же, как оно противодействует иным военным угрозам, а именно, системно. Из статьи Линна можно понять, что для создания абсолютного военного превосходства в киберпространстве в Пентагоне подготовлен целый комплекс программ, который призван решить множество специфических проблем.

Американским вооруженным силам понадобятся новые технические средства – сенсоры, новые аналитические инструменты, автоматизированные системы управления. И дело не только в количественном превосходстве технических средств, но и в их качестве, а также в эффективности их применения. Очевидно, что все они будут доступны для Пентагона только в том случае, если будут соответствовать современным требованиям кибербезопасности, а именно, если, во-первых, именно американская промышленность информационных технологий (коммерческий сектор) останется основным, причём конкурентоспособным поставщиком такого рода техники (иначе говоря, сохранит

* Принята в ноябре 2010 года.

мировое лидерство в области информационных технологий – ИТ); и во-вторых, если будет радикально обновлён специальный механизм приобретения ИТ для военных целей.

В этом контексте лидерство американского ИТ-бизнеса становится приоритетной проблемой национальной обороны США, на решение которой направляются весьма значительные ресурсы, находящиеся в распоряжении государства. Более того, Пентагон привлекает к борьбе с киберугрозами и крупные компании. Создан специальный государственно-частный Институт сотрудничества (*Enduring Security Framework)*, в рамках которого руководители ИТ-подразделений коммерческих компаний встречаются с представителями Министерства обороны, а также Министерства внутренней безопасности и Управления национальной разведки.

У. Линн подчеркивает, что тематикой кибербезопасности активно занимаются ведущие военные научно-исследовательские институты и обращает внимание на скорое появление важной инновационной программы Национальное киберпространство (*National Cyber Range*), разработанной специалистами Агентства передовых оборонных разработок (*DARPA*), несколько десятилетий назад участвовавшего в создании Интернета. Ключевой особенностью этой программы станет уникальная модель симулирования кибервойны в Интернете, которая должна позволить военным тестировать те или иные средства и методы кибероборонbы до их «постановки на боевое дежурство». Здесь уместно упомянуть, что, следуя опыту коммерческих компаний, системные администраторы действующих военных коммуникационных сетей проходят подготовку по специальному проекту «Этический хакинг» (*ethical hacking*), в рамках которого известные вредоносные программы потенциальных противников используются для тестирования американских информационных сетей с целью заблаговременного выявления их уязвимых мест. В статье отмечается, что такое моделирование, позволяющее подробно изучить особенности распространения и свойства вирусных программ различной природы, поможет Соединённым Штатам опередить противников в области наступательного кибероружия.

Что же касается механизма приобретения информационных технологий, то, по мнению Линна, он должен опираться на четыре взаимосопряженных принципа:

1) *Время, которого требуют процедуры заказа, создания и внедрения информационных технологий* (снизу до верху) – от низовых войсковых подразделений до стратегического командования и центрального аппарата МО – *должно соответствовать реальному циклу обновления таких технологий, т.е. составлять от 12 до 36 месяцев*, а не семь–восемь лет, что типично для сформировавшихся в настоящее время бюрократических процедур оформления и реализации государственных заказов и контрактов на вооружения и военную технику. Сейчас для внедрения той или иной инновационной компьютерной системы, с учётом времени, необходимого для принятия решения о финансировании её создания, Пентагону требуется в среднем 81 месяц. *Это более чем в 3 раза дольше срока создания популярного гаджета* iPhone. Такое отставание просто небезопасно, поскольку согласно закону Мура*, к моменту внедрения такой системы в прак-

* Закон Мура – удвоение мощности интегральных схем каждые полтора-два года.

тическую деятельность Министерства обороны, они устаревают как минимум на четыре поколения по сравнению с гражданскими моделями, которые могут быть доступны потенциальному противнику.

2) Необходимо *в максимально возможной степени* отказаться от «специальных заказов» на разработку ИТ, и *использовать стандартные* (коммерческие) *технологии*.

3) *Все информационные системы должны быть совместимы и взаимоувязаны (интегрированы)*, несмотря на то что реальные потребности МО в области информационных систем очень широки и разнообразны: они простираются от модернизации систем управления обычным и ядерным оружием до аналитических систем фильтрации разведывательных данных различной природы и сложности.

4) Необходимо избегать одновременного введения в эксплуатацию каких-либо сверхсложных информационных систем и *внедрять различные модульные элементы поэтапно, поддерживая таким образом военную информационную инфраструктуру в состоянии перманентной модернизации и обновления*.

Особенное внимание американское государство, по мнению У. Линна, должно уделять подготовке кадров в области кибербезопасности. Пентагон продолжает привлекать большое количество таких специалистов, постоянно повышает их квалификацию. Сегодня программа сертификации специалистов охватывает в три раза больше специалистов, чем несколько лет назад.

Оценивая в целом идеи У. Линна необходимо подчеркнуть, что они безусловно интересны не только для американских военных, но и для русских специалистов, занятых проведением военной реформы, а также обеспечением информационной безопасности России.

Список литературы

1. *Глазьев Сергей*. Мировой экономический кризис как процесс доминирующих технологических укладов ((http://www.glazev.ru/scienexpert/84/).

2. *Роговский Е.А.* Лидерство США в глобальных технологиях и международная безопасность // США ❖ Канада. 2007. № 9. С. 53–70.

3. *Gorman S., Cole A., Dreazen Y.* Computer Spies Breach Fighter-Jet Project // Wall Street Journal. 21.04.2009 (http://online.wsj.com/article/SB124027491029837401.html#printMode).

4. *Lynn William J.* Defending a New Domain: The Pentagon's Cyberstartegy // Foreign Affairs. September/October 2010.

5. *McConnell M.* 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).

6. *Nakashima E.* Pentagon's Cyber Command Seeks Authority to Expand Its Battlefield // Washington Post Saturday, November 6, 2010 http://www.washingtonpost.com/wp-dyn/content/article/2010/11/05/AR2010110507304_pf.html