УДК 321.01.(066)

© Микрюков В.Ю.
Mikrjukov V.

ИНФОРМАЦИОННЫЕ ВОЙНЫ

INFORMATION WARFARES

Аннотация. *Проанализированы особенности войн с использованием информационных технологий.*

Annotation. *Warfares with use of information technologies are analysed.*

Ключевые слова. *Информационная война, информационная технология, информационное превосходство, информационное оружие, кибервойна, сетецентрическая война.*

Key words. *information warfare, information technologies, the information superiority, the information weapon, cyber-warfare, network-centric warfare.*

По мнению западных специалистов, современная война – это информационная война, и её выигрывает тот, чьи информационные системы более совершенны. «Компьютеры – это оружие, а линия фронта проходит повсюду», - пишет американский военный аналитик Джеймс Адамс в книге «Следующая мировая война». А сам термин «информационная война» появился в середине 80-х годов прошлого века в связи с новыми задачами вооружённых сил США после окончания «холодной войны» (разработка группы военных теоретиков США в составе Г. Экклз, Г. Саммерз и др.) и начал активно употребляться после проведения операции «Буря в пустыне» в 1991 году, когда новые информационные технологии впервые были использованы как средства ведения войны многонациональных сил США и их союзников против Ирака.

В ноябре 1991 г. американский генерал Гленн Отис опубликовал работу, в которой прямо указывалось: «Из операции «Буря в пустыне» можно извлечь много уроков. Некоторые из них – новые, другие – старые. Один урок, однако, является поистине фундаментальным: природа войны коренным образом изменилась. Та сторона, которая выиграет информационную кампанию, - победит. Мы продемонстрировали этот урок всему миру: информация является ключом к современной войне – в стратегическом, оперативном, тактическом и техническом отношениях» [10]. Вскоре после этого термин «информационная война» был официально закреплён в директиве Министерства обороны США (21 декабря 1992 г.).

В настоящее время в военных кругах США под информационной войной понимаются действия, предпринимаемые для достижения информационного превосходства в поддержке национальной военной стратегии посредством воздействия на информацию и информационные системы противника при одновременном обеспечении безопасности и защиты собственных подобных систем.

Оценка основных направлений ведения подобной войны подтверждается выделением в программах Университета национальной обороны США таких форм информационного противоборства, как РЭБ, война с использованием средств разведки, психологическая и кибернетическая, борьба с хакерами.

Исследуя информационные войны, американские аналитики вводят понятие информационного превосходства - возможность сбора, обработки и распространения непрерывного потока информации при воспрещении использования (получения) ее противником. Сегодня подобные операции играют существенную роль в достижении военного превосходства. Американцы в своей концепции ставят вопрос об усилении работы по объединению информационных операций в самостоятельный вид боевых действий наряду с другими операциями вооружённых сил (от физического устранения до психологической операции против систем защиты компьютерных сетей). В этом контексте отдельно рассматривается проблема оценки военного ущерба, нанесённого противнику такими операциями. Более того, оценивая их как перспективный самостоятельный вид боевых действий (за счёт которого в Пентагоне и рассчитывают в будущем добиваться решающих результатов), командование ВС США предполагает введе-

Василий Юрьевич Микрюков – доктор педагогических наук, кандидат технических наук, профессор, Академия военных наук, тел. 8(495)543-36-76.

Mikryukov Vasily – doctor of education, Ph.D., professor, Academy of Military sciences, tel. 8 (495) 543-36-76.

ние в виды вооружённых сил соответствующих формирований, укомплектованных специалистами, получившими специальную подготовку и оснащёнными современным информационным оружием.

Информационное оружие — это средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним законных пользователей, дезорганизации работы технических средств, вывода из строя телекоммуникационных сетей, компьютерных систем, всех средств высокотехнологического обеспечения жизни общества и функционирования государства.

Особую опасность информационное оружие представляет для компьютерных систем органов государственной власти, управления войсками и оружием, финансами и банками, экономикой страны, а также для людей при информационно-психологическом (психофизическом) воздействии на них с целью изменения и управления их индивидуальным и коллективным поведением.

Информационное оружие может быть использовано для инициирования крупных техногенных катастроф на территории противника в результате нарушения штатного управления технологическими процессами и объектами, имеющими дело с большими количествами опасных веществ и высокими концентрациями энергии. При этом по своей результативности оно сопоставимо с оружием массового поражения.

Определяя особенности информационной войны, эксперт по безопасности правительства США Ричард А. Кларк вводит понятие «кибервойна». По его определению «кибервойна — действия одного национального государства с проникновения в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения». Американский журнал «Экономист» описывает кибервойну как «пятую область войны, после земли, моря, воздуха и космоса».

Кибервойна, по взглядам американского армейского руководства, основана на киберразведке, кибератаках и киберобороне, проводимых в киберпространстве.

Под киберпространством американскими военными стратегами понимается «глобальный домен в пределах информационного пространства, состоящий из взаимозависимой сети информационных технологических инфраструктур, включая Интернет, телекоммуникационные сети, компьютерные системы, а также встроенные в них процессоры и контроллеры» [13].

Киберпространство формируется взаимосвязанными компьютерными системами и системами передачи данных, которые хранят, обрабатывают и передают разнообразную информацию с использованием программных и аппаратных средств. Оно создается, поддерживается и эксплуатируется частными и государственными субъектами, существующими по всему миру. Характерными особенностями киберпространства, отличающими его от традиционных геофизических видов пространств ведения военных действий, являются его искусственное происхождение, инновационность и изменчивость [5].

Основу операций, проводимых в киберпространстве, составляют кибератаки, которые используются для того, чтобы «уничтожать, искажать, модифицировать, разрушать информационные ресурсы, компьютеры, коммуникационные системы, встроенные процессоры и контроллеры противника и, таким образом, снижать эффективность принятия ими решений» [5].

С началом кибервойны в первую очередь будут предприняты кибератаки на компьютерные системы и серверы командных пунктов управления, государственных учреждений, финансовых и деловых центров. Эти атаки будет подкреплены активацией компьютерных вирусов, прежде всего «троянских коней», «заложенных» в ЭВМ противника ещё в мирное время. Помимо этого, предполагается использовать специальные устройства, которые при взрыве создают мощный электромагнитный импульс или биологические средства наподобие особых видов микробов, способных уничтожать электронные схемы и изолирующие материалы в компьютерах.

Будут проводиться информационные диверсии с целью несанкционированного доступа к базам данных, нарушения линий связи, хищения и копирования информации, её сокрытия и искажения.

Эффективность хакерских атак показал случай, произошедший в США в 1988 г. Тогда американский студент Р. Моррис «запустил» через Интернет вирус, который на три дня (с 2 по 4 ноября 1988 г.) вывел из строя фактически всю компьютерную сеть США. Были парализованы компьютеры Агентства национальной безопасности, Стратегического командования ВВС США, локальные сети всех крупных университетов и исследовательских центров. Лишь в последний момент удалось спасти систему управления полётом космических кораблей Шаттл. Ущерб оценивался более чем в 100 миллионов долларов.

В 2008 г. через Интернет была взломана информационная система Пентагона и выведены из строя около 1 500 компьютеров. Американские официальные лица утверждали, что эта вирусная атака под названием «Титановый дождь» проводилась под покровительством властей Китая. В январе 2009 года истребители ПВО ВМС Фран-

ции в течение нескольких дней не могли подняться в воздух по причине заражения компьютеров самолетов вирусом Downadup. Вирус использовал уязвимость в операционной системе Windows, и при этом было невозможно загрузить планы полётов [2].

В 2010 г. атакам через Интернет подверглись 53% организаций и промышленных предприятий, в том числе свыше 20 крупнейших компаний, таких, как Google, Yahoo, Symantec, Adobe и другие. Средний ущерб от таких действий, с учетом того, что по оценкам экспертов 3 из 5 атак являются успешными, составил порядка 850 тыс. долларов США [2]. Последний инцидент с материалами бывшего сотрудника ЦРУ и Агентства национальной безопасности США Эдварда Сноудена и сайта WikiLeaks только подтвердил уязвимость различного рода информационных систем, несовершенство механизмов их защиты и законодательства в информационной сфере.

Уже сегодня, по заявлениям некоторых иностранных экспертов, отключение компьютерных систем приведёт к разорению 20% средних компаний и около 33% банков в течение нескольких часов, 48% компаний и 50% банков потерпят крах в течение нескольких суток [8]. В результате будет обрушена экономика государства.

В специфическом плане агрессоры могут использовать шпионаж и проникновение в сети, чтобы внедрить вирусы типа «троянского коня, логической бомбы», которые могут оставаться бездействующими и необнаруженными до определённого времени и нужных обстоятельств. Активация этих «бомб замедленного действия» позволила бы агрессору быстро взять под свой контроль определённую систему прежде, чем жертва узнала бы о проникновении в неё. Эти действительные нападения, если они координируются, могут нанести существенный урон в определённое время или в месте политической напряженности и служить прелюдией к обычной войне [7].

Одна из главных особенностей киберпространства – анонимность агрессора. В случае возникновения подозрения в том, что кибератака спонсируется государством, трудно установить, что заказчиком является глава государства или правительство. Используя ложные IP-адреса, иностранные серверы и псевдонимы, агрессор может действовать с почти полной анонимностью и относительной безнаказанностью.

Поэтому в кибервойне чрезвычайно трудно прямое точное и пропорциональное применение силы; цель может быть военной, промышленной или гражданским лицом или это может быть помещение с сервером и большим количеством клиентов, и только у одних среди них есть намеченная цель.

Хотя у государства есть намного больший доступ к киберпространству, всё же большая часть этого пространства находится в частных руках. Оружие кибервойны почти всегда имеет двойное назначение, и физические аппаратные средства могут быть применены и для военных, и для гражданских целей. При этом противника почти невозможно идентифицировать и поэтому удержать. Поскольку Интернет продолжает развиваться, то киберпространство постоянно меняется и имеет тенденцию к расширению. При этом анонимные агрессоры динамичны и редко обнаруживаются, тогда как статические защитники должны успешно парировать каждый их удар.

Следовательно, любому государству нужно не только скрупулезно готовить кибератаки, но и не менее тщательно организовывать кибероборону.

С 2010 до 2015 гг. американское правительство планирует потратить более чем 50 млрд. долларов на кибероборону. В эту сумму не входят затраты промышленных и торговых предприятий для защиты от киберугроз. При этом расходы увеличиваются, когда эти угрозы становятся более очевидными.

Масштаб американского военного использования киберпространства обширный. Есть 15000 сетей Министерства обороны с семью миллионами устройств (4 000 установок в 88 странах). Эти системы просматриваются и исследуются миллионами потенциальных агрессоров каждый день [4]. Между октябрем 2008 г. и апрелем 2009 г. Пентагон официально потратил свыше 100 миллионов долларов на восстановление повреждений, вызванных кибератаками. Фактически эти расходы значительно выше [6].

Наступательное действие в кибервойне легче, быстрее и дешевле, чем защитное. Так, ежегодный оборонный бюджет США составляет приблизительно 700 млрд. долларов. Но согласно одному американскому кибераналитику безопасности, для того, чтобы подготовить кибератаку, которая выведет из строя компьютеры и парализует Соединённые Штаты, потребовалось бы два года и менее 600 человек, а стоило бы это меньше, чем 50 млн. долларов в год [3].

В связи с этим возникает вопрос: может быть, вместо того, чтобы тратить огромные средства на разработку и производство вооружения и военной техники, в том числе и оружия массового поражения, может стоить обучать программистов и готовить батальоны хакеров и антихакеров?

Ответ на данный вопрос неоднозначен.

Во-первых, кибератака обычно не является прямой (в смысле физического нападения, предпринятого, например, чтобы разрушить промышленный объект или транс-

портный), но разрушает информацию и сети коммуникации, вызывая желательный эффект косвенными средствами. При этом ни нападающий, ни защитник не знают полную степень уязвимости сети (ей) и затронет ли нападение другие связанные сети [7].

Во-вторых, управление их задачами будет трудным: результат целой кампании может зависеть от тактического (но политически и стратегически жизненно важного) результата – например, перестрелка в критической части критического поля битвы. Как может командир взвода пехоты, прижатой огнём артиллерии, запросить киберпомощь, чтобы нейтрализовать артиллерийский огонь с помощью компьютеров? [7]/

В кибервойне особенно трудно сдержать противника. Сдерживание основывается на вероятных гарантиях того, что у обороняющегося есть возможность наказать агрессора; и эта способность должна быть сообщена противнику, которого следует ещё и опознать. Но бывший советник президента США по вопросам кибербезопасности Ричард Кларк спрашивал по этому поводу: «как сдержать противника от кибервойны, когда наши средства и способы являются секретными и наше оружие непродемонстрировано?» [7].

Отличительной особенностью кибервойны является стремительность, с которой она может развиться. По мнению бывшего директора ЦРУ Майкла Хайдена, «киберугроза двигалась настолько быстро, что мы были всегда в опасности создания прецедента прежде, чем мы подстроим политику», темп изменения может быть столь резким относительно обычного, цикл действия ответной реакции стратегически устаревал прежде, чем она начиналось: как будто правительство послало эксплуатационного аналитика, чтобы пронаблюдать эффект применения в сражении замка кремневого ружья, чтобы обнаружить по прибытию, что уже изобретён пулемёт Максима [7].

Гонка вооружений предопределяет гонку вооружений в киберпространстве. Сталкиваясь с быстрым развитием киберугроз, правительства многих стран стремятся достигнуть более быстрого ответа на это развитие.

Так, Пентагоном поставлена цель завоевания военно-стратегического превосходства США в мировом киберпространстве: «США должны располагать превосходством в киберпространстве, чтобы обеспечить себе свободу действий и одновременно лишить этого наших противников...» [15].

Понимая всю важность информационного противоборства, еще в июне 2009 г. в США было создано киберкомандование, на которое возложена ответственность за безопасность компьютерных сетей Министерства обороны США, ведение компьютерной разведки, предотвращение кибератак на США и нанесение упреждающих ударов по противникам, готовящим подобные акции. В настоящее время сформированы 24-я кибернетическая армия ВВС и 10-й киберфлот ВМС. Около 10000 специалистов по кибербезопасности трудятся в Центре стратегических и международных исследований в рамках программы US Cyber Challenge.

Кроме США, ещё около 100 стран мира имеют в составе вооружённых сил подразделения для проведения операций в киберпространстве.

Другой концепцией вооружённой борьбы будущего, в основе которой лежит использование информационных технологий, стала концепция «сетецентрической войны». Эта концепция была разработана в конце 90-х годов прошлого века военными теоретиками США А. Себровски и Дж. Гарстка.

В основе сетецнтрической войны (СЦВ) – увеличение суммарной боевой мощи воинских формирований путём соединения их в единую сеть, для которой характерны две основных характеристики: быстрота управления и самосинхронизация. Быстрота управления достигается за счёт информационного превосходства путём внедрения новых систем управления, слежения, разведки, контроля, компьютерного моделирования. В результате противник лишается возможности проводить эффективные операции, так как все его действия будут запаздывать. Под самосинхронизацией подразумевается способность организационной структуры воинских формирований, форм и методов выполнения ими боевых задач видоизменяться по своему усмотрению, но в соответствии с потребностями вышестоящего командования. В результате военные действия приобретают форму непрерывных высокоскоростных действий (операций, акций) с решительными целями.

Таким образом, сеть позволяет географически рассредоточенные силы (относящиеся к разным видам и родам войск) объединить в едином замысле операции и за счёт информационного превосходства использовать эти силы с большей эффективностью путём обеспечения единства взглядов командующих (командиров) разнородных войск (сил) на содержание, роль и место взаимодействия в операции, а также путём самосинхронизации своих действий в интересах достижения общей цели операции.

Преимущества СЦВ [1]:

1. *Использование географически рассредоточенных войск (сил).* В прошлом это ограничивало боевые возможности из-за необходимости организации связи рассредоточенных войск, их выдвижения к месту сосредото-

чения, определения необходимого состава сил и вооружения и др. Свои ограничения накладывали пути сообщения, по которым выдвигались войска для совместных действий, коммуникации войск, различные системы боевого управления разнородных войск (сил), различное техническое обеспечение взаимодействующих войск. Технологии века информации решили многие эти вопросы, освободив географически рассредоточенные войска от необходимости двигаться к месту сосредоточения в целях совместного выполнения боевых задач. Это уменьшает риск поражения войск на марше и лишает противника возможности определить цель проводимых операций и направление главного удара. Кроме того, расширяется возможности привлечения к проводимым операциям дополнительных сил и средств, сокращаются объём и время транспортных перевозок боеприпасов, материальных и технических средств.

2. *Увеличенная скорость и объём передаваемой информации и значительно улучшенный доступ к ней.* Это обеспечивается тем, что средства добывания и передачи информации о целях и средства поражения целей могут находиться в географически удалённых местах без необходимости их перемещения поближе друг к другу.

3. *Оперативность обработки информации и принятия решений.* Сеть – это не просто средство для передачи «информации и команд» от одного места к другому, но и технологическая область по обработке информации и выработке решений. Эффективность боевых действий во многом зависит не только от своевременного получения достоверной и полной информации, но и от её правильной и быстрой обработки, позволяющей превратить информацию о боевых действиях в знание того, как действовать в сложившихся условиях обстановки.

4. *Самосинхронизации*. Хорошая информированность командующих (командиров) взаимодействующих войск (сил) о целях, задачах и ходе операций позволяет им самосинхронизировать свои силы и действовать автономно, но в рамках единого замысла. В свою очередь, это позволяет скрытность выполнения боевых задач и высокую эффективность их выполнения. Управление взаимодействующими войсками (силами) может быть распределено по поставленным задачам и динамически перераспределяться в зависимости от складывающейся обстановки, что обеспечивает гибкость управления, возможность использовать широкий диапазон управляющих действий от общепринятых до инновационных, таких как самосинхронизация.

Таким образом, СЦВ отражает и включает все особенности, необходимые для успеха в веке информации: способность объединять боевые возможности географически рассредоточенных сил в операциях без их сосредоточения в одном месте (на одном плацдарме), оперативность обработки информации и значительно улучшенный доступ к ней, гибкость управления взаимодействующими войсками (силами) от централизованного управления до автономного (самосинхронизация) [1].

Устранение географических ограничений позволило перейти от подхода, основанного на сосредоточение войск (сил) к подходу, основанному на акцентировании эффектов. СЦВ, объединяя силы, учитывает и важность центра – взаимодействие командующих (командиров), что является необходимым, чтобы произвести синергетические эффекты. В целом у СЦВ есть всё необходимое для того, чтобы осилить важнейшую особенность войны – её динамическую природу [1].

К 2025 г. в ВС США планируется создание единой информационной разведывательно-ударной системы, функционирующей в едином информационном «сетецентрическом» пространстве. Создание системы подразумевает внутреннюю интеграцию ВС, укрепление связей с другими федеральными агентствами, максимальную децентрализацию войск под выполнение конкретных задач, их адаптацию к конфликтам любого масштаба, «сетецентричность» и подавляющее информационное превосходство во всех сферах возможного противоборства: воздушной и космической, наземной, морской и киберсфере [9].

Критика теории сетецентрической войны касается, в первую очередь, перекоса в сторону технологий, и авторы критики вполне справедливо замечали, что в центре войны по-прежнему остаётся человек, его воля, и «война не «сетецентрична». Она или «человекоцентрнчна», или у нее нет какого-либо центра вообще» [12]. «Несмотря на огромные выгоды от использования сети, это было бы безумие терять из виду тот факт, что сеть – просто инструмент, призванный помочь командующему в процессе выработки и принятия решения. Мы – командноцентрпчные вооруженные силы, использующие сети» [16].

Большой поток критики сетецентрического подхода был связан с военной кампанией Израиля против террористической организации «Хезболла» в Ливане в 2006 г. и военной операцией США «Иракская свобода» в 2003 г.

В аналитических материалах, оценивающих действия Армии обороны (АО) Израиля отмечается, что доктрина АО недооценила тот факт, что дистанционное командование и управление при всех возможностях и преимуществах никогда не сможет заменить собой роль командира в реальном бою, которая, как и прежде, остается критичной. Новые возможности, безусловно, полезны для закрытого обмена информацией на высших уровнях во-

енного командования, однако они не могут использоваться для дачи приказов командирами тактического звена на поле боя, когда критически важным становится голос командира и общий эфир, обеспечиваемый радиосетями. В условиях реального боя голос командира, его спокойствие и владение ситуацией, был и остается незаменимым [11].

Согласно офицеру резервисту Рон Тира, новая доктрина смещала «фокус» на когнитивную сторону войны и медиавойну: «Вместо того чтобы убивать плохих парней, как это было в старые добрые времена, они хотели создать «сознание победы» на нашей стороне и «когнитивное восприятие поражения» на другой». Сложная, непривычная терминология новой доктрины на 170 страницах была усвоена и использовалась высшим командным составом вплоть до уровня дивизии, в то время как тысячи офицеров нижнего тактического звена предпочитали использовать старую. Командиры, непосредственно работающие с личным составом, должны говорить в простой доступной манере, которая выстраивается вокруг двух вещей - что мы должны захватить и что разрушить» [14].

Тем не менее, несмотря на критику, мировой опыт военного строительства свидетельствует, что обеспечение всесторонней интеграции систем управления, связи, поражения и всестороннего обеспечения, повышение уровня их взаимодействия, а также достижение синергетического эффекта за счет создания сетецентрических связей становится приоритетным направлением реформирования ВС большинства стран мира.

Уже сейчас ясно, что информационное противоборство является тем фактором, который оказывает существенное влияние на саму войну. Государства будут решать все свои проблемы не с помощью группировок войск на базе живой силы, а путём завоевания информационного превосходства.

В вооружённой борьбе победа может быть достигнута за счёт информационной операции, в результате которой будет разрушен экономический потенциал противника. В условиях разрушенной экономики вооружённые силы обречены сначала на потерю боеспособности, а затем и на полный развал. В таких условиях неизбежно рухнет и политический строй.

Так было в ходе вооружённого конфликта в Ливии в 2011 г., когда коалиционными силами НАТО были блокированы сетевые информационные ресурсы правительства Муаммара Каддафи и осуществлён контроль над управляемой через Интернет инфраструктурой жизнеобеспечения и банковской системой страны.

Литература

1. Албертс Д., Гартска Дж., Штейн Ф. Сетецентрическая война: развитие и усиление информационного превосходства. Вып. 2, перераб. КИП, 2000.

2. Антонович П.И. О современном понимании термина «кибервойна»//Вестник Академии военных наук, 2011.- № 2. – С. 91.

3. Гражданин Оттавы, 2010. - 18 июня 2010 -http://www.ottawacitizen.com/news/Time+wake+cyber+threat+Experts/3170415/story.html.

4. Джексон У. Министерство обороны изо всех сил пытается определить кибервойну: усилия, которым препятствует нехватка соглашения по значению/Правительственные Компьютерные Новости, 2010. - 12 мая. http://gcn.com/articles/2010/05/12/miller-on-cyberwar-051210.aspx.

5. Дылевский И.Н. и др. Операции в киберпространстве: вопросы теории, политики, права//Военная мысль, 2011. - № 8. – С. 72.

6. Индепендент, 2009. - 8 апреля. - http://www.independent.co.uk/news/world/americas/pentagonspends-big-fixing-cyber-attack-damage-1665728.html.

7. Корниш П. и др. На Кибервойне. - Королевский Институт Международных отношений, 2010. - www.chathambouse.org.uk.

8. Матвиенко Ю. Предупредить - значит вооружить/Информационно-аналитический портал Геополитика. - http://www.geopolitica.ru/Articles/1199.

9. Налетов Г.А. К вопросу о разработке концепции нетрадиционных войн и вооружённых конфликтов//Вестник Академии военных наук, 2012. - № 1. – С. 31.

10. Adams J. The Next World War. Computers Are the Weapons and the Front Line Is Everywhere. New-York, 1998. - P. 55.

11. Esbel D. Winograds Blessing in Disguise: Last Wake up Call for Israel//in Defense Update online bi-monthly defense magazine, 2008.

12. Giffin, Ralph E. and Darryn J. Reid. A Woven Web of Guesses, Can to One: Network Centric Warfare and the Myth of the New Economy. unpublished manuscript, Australian MoD. – PP. 2-5.

13. Joint Operations, Joint Publication 3-0.17 September 2006. Incorporating (Change 2, 22 March 2010. The U.S. Army's Cyberspace Operation Concept Capability Plan 2016-2028. Training and Doctrine Command (TRADOC) Pamphlet (Pam) 525-7-8, 22 February 2010; Cyberspace Operations. Air Force Doctrine Document (AFDD) 3-12, 15 July 2010.

14. Matthews M. We Were Caught Unprepared: The 2006 Hezbollah-Israeli War. Long War Series Occasional Paper 26, U.S. Army Combined Arms Center, Combat Studies Institute Press, Fort Leavenworth, Kansas, 2008. – PP. 27-28.

15. The National Military Strategy for Cyberspace Operations, Joint Chiefs of Staff, Washington, D.C., December, 2006.

16. Wallace W.S. Network-enabled battle command//Military Review, 2005. – Vol. 85. - №. 3.

Материал поступил в редакцию 12. 02. 2014 г.