**Содержание**

Введение...................................................................................................................3

1. Китайская специфика в ведении информационной войны.............................4

3. США в сфере информационной безопасности.................................................7

Заключение.............................................................................................................12

Список литературы................................................................................................14

**Введение**

В современном деловом мире происходит процесс миграции материальных активов в сторону информационных. По мере развития организации усложняется ее информационная система, основной задачей которой является обеспечение максимальной эффективности ведения бизнеса в постоянно меняющихся условиях конкуренции на рынке.

По данным ФАПСИ, расходы США за последние 15 лет на разработку и приобретение средств информационной борьбы выросли в 4 раза и занимают ныне первое место среди расходов на все военные программы. В 2006 году в ФАПСИ подготовили и опубликовали аналитическую справку под броским названием "Информационное оружие как угроза национальной безопасности России". В результате в 2007 году Госдума, а затем Межпарламентская ассамблея СНГ обратились в ООН, ОБСЕ и Совет Европы с предложением о принятии международной конвенции о запрещении информационных войн и ограничении оборота информационного оружия. В марте 2008 года этот вопрос был поднят на встрече с генсеком ООН и по инициативе России включен в повестку Генеральной ассамблеи ООН[[1]](#footnote-1).

 Кроме ФАПСИ, информационным оружием живо заинтересовалось Минобороны, рассчитывая увеличить оборонный заказ на разработку подобных средств. В результате лоббирования со стороны силовых структур Государственная комиссия по военному строительству РФ включила средства информационной борьбы в состав трех приоритетных факторов отечественного потенциала сдерживания возможной агрессии извне (наравне со стратегическими ядерными силами и системами высокоточного оружия).

**1. Китайская специфика в ведении информационной войны**

Исследуя стратегию действий Китая, а также роль и место в ней средств и методов информационной войны эксперты столкнулись с рядом фундаментальных отличий, корни которых лежат в культурном различии Западной и Восточной цивилизаций. По мнению специалистов наиболее рельефно отражают различия в менталитете народов древнейшие логические игры, получившие широкое распространение и признание на Востоке и на Западе: для Запада это шахматы, а для Востока — игра го[[2]](#footnote-2). Шахматы предполагают наличие полного комплекта фигур до начала поединка, в то время как партия го начинается с чистого игрового поля. В процессе игры в шахматы силы противников убывают, пропорционально утрате отдельных фигур, вместо этого в го силы одного из противников увеличиваются за счет установления контроля над фигурами другого противника. Чем больше длится партия в го, тем чувствительнее становятся позиции противников к ошибкам, тем значительнее становятся преимущества того, кто первый сможет воспользоваться ошибкой противника. Итог шахматной партии – разгром армии противника и гибель короля, при этом, как правило, серьезно страдает и собственная армия, итог же партии го – установление контроля над большей частью территории игрового поля, причем сила победителя тем больше, чем была больше сила противника. Важным итогом этой аналогии является осознание сути восточной стратегии противоборства: в стратегии нужно стремиться к большему влиянию при минимальных затратах при этом не уничтожать противника и собственную нацию в бесконечной борьбе, а использовать ресурс и возможности противника для собственного роста.

Важным является то, что главной целью остается не победа над противником любой ценой, даже ценой его полного истребления, но, избегая непосредственных столкновений и стратегических перемещений сил, достижение господства, выживания и процветания собственного народа. Этот подход оставляет жизнеспособной нацию, позволяя ей доминировать над процветающим миром, а не над миром разрухи, негодования и бедности.

Великая стратегия Китая в полном объеме остается закрытой от широкой публики, однако наибольший интерес, по мнению американских экспертов, представляет именно интерпретация китайского «ши», так как в отношении этого термина отсутствует какой-либо западный эквивалент. Лингвисты трактуют его как «выравнивание сил», «склонность вещей» или «потенциал, рожденный диспозицией», который в руках высококлассных стратегов может гарантировать победу над превосходящей силой[[3]](#footnote-3).

Осознание базовых принципов китайской стратегии позволяет экспертам утверждать, что сегодня в Китае может превалировать совсем иное представление о США как о глобальном противнике. Наиболее вероятно, что, базируясь на культурных различиях и «стратегии го», Китай видит Соединенные Штаты как препятствие к достижению контроля и влияния в регионе и в мире в целом, однако победа Китая над этим противником не возможна без использования ресурса самого противника. Учитывая безусловные выгоды во взаимодействии с Соединенными Штатами — прежде всего в вопросах торговли и технологий – Пекин, очевидно, полагает, что Соединенные Штаты представляют существенный долгосрочный вызов. Руководство Китая утверждает, что Соединенные Штаты стремятся поддерживать доминирующее геостратегическое положение, сдерживая рост китайской мощи, и, в конечном счете, их стремление будет направлено на расчленение и «вестернизацию» Китая, одновременно не допуская возрождения России. Кроме этого Китай отрицательно относится к взаимоотношениям США с Японией и Тайванем.

Эксперты полагают, что версия о том, что Китай в настоящее время ведет информационную войну «незападной» формы получает достаточно много подтверждений. Так, в последнее время Китай стремится накапливать как можно больше значащей информации (особенно в области экономики и обороны), защищать собственную информацию, лиц принимающих решения и национальное единство. Китайцы стремятся эксплуатировать информационные системы их противника, создают общественные структуры, пытаясь влиять на процесс принятия решений их противником. При этом Китай пробует скрыть свои собственные намерения от Запада, потому что китайские стратеги осознают преимущества такого положения: возможность эксплуатации намного больше, когда цель предпринимаемых действий не осознается противником.

Анализ открытой китайской литературы позволил экспертам выделить ряд базовых положений китайской концепции информационной войны. К ним относят: атаки на компьютерные сети, информационные операции, экономические операции, высокоточные удары и направленные акции. Среди наиболее часто описываемых целей возможной войны было идентифицировано пять: преимущество национальной безопасности, экономическое преимущество, финансовая выгода, политическое влияние и изменение политики. В перспективе можно ожидать тесного переплетения всех четырех инструментов национальной мощи: вооруженных сил (преимущество национальной безопасности), экономики (финансовая выгода), дипломатии/политики (изменение политики) и информации (политическое влияние). Таким образом, любые средства, которые увеличивают национальную мощь, рассматриваются китайскими стратегами в качестве средства противоборства[[4]](#footnote-4).

Понимание американскими экспертами китайского подхода к концепции информационной войны в академических кругах и сообществах экспертов остается сегодня недостаточным для построения адекватной стратегии противодействия Китаю в информационной сфере в ближайшие годы.

**2. США в сфере информационной безопасности**

В настоящее время ФБР совместно с АНБ ведут работы по созданию системы контроля за электронной почтой в Интернет. На программу технического перевооружения АНБ "GroundBreaker" Конгресс выделил свыше 5 млрд. долл. и еще около 1 млрд. долл. дополнительно на переоснащение многоцелевой атомной подводной лодки класса  "Sea wolf" для прослушивания подводных кабелей связи с помощью специальной аппаратуры. Названная в честь президента США Джими Картера новая субмарина SSN-23 должна была быть спущена на воду в декабре этого года, но по настоянию АНБ было принято решение провести ее переоборудование, а спуск лодки отложить до июня 2009 г. По сведениям, просочившимся в печать, после ввода в строй новой субмарины АНБ рассчитывает прослушивать не только обычные электрические кабели связи, что оно делало и раньше, но и … волоконно-оптические! Как это удастся сделать американцам - пока не ясно: для бесконтактного перехвата экранированного светового луча еще не придуман способ. Между тем, подводная лодка-шпион будет нести на своем борту специальный контейнер-камеру, из которой может быть осуществлен беспрепятственный доступ к любым подводным объектам[[5]](#footnote-5).

Ежегодно США расходуют на информационные технологии только из федерального бюджета порядка 38 млрд. $, из которых около 20 млрд. $ (более 50%) составляют расходы военного ведомства.  И это без учета десятков млрд. $. затрачиваемых на бортовые системы управления спутников, ракет, самолетов, танков и кораблей. Сегодня Пентагон это не только один из крупнейших владельцев, арендаторов и пользователей информационных и телекоммуникационных ресурсов, ведущих заказчиков программного обеспечения, компьютерного оборудования и средств цифровой связи, но и, по сути дела, законодатель государственной политики и промышленных стандартов в области информационной безопасности. Только в 2007 г. на защиту национальных информационных ресурсов в  США было выделено 1,5 млрд. $, в то время как Пентагон истратил на защиту военных информационных систем 1,1 млрд. $.

В определенной степени это сказывается и на самих понятиях, связанных с защитой информации, которые постепенно трансформируясь из чисто военных терминов приобретают характер общегосударственных и промышленных стандартов. Производители оборудования и разработчики программных продуктов, заинтересованные в крупных государственных и военных заказах, начинают прислушиваться к тому, что говорят в коридорах Пентагона об информационной безопасности[[6]](#footnote-6).

Осознав на собственном опыте бессмысленность защиты информационных ресурсов без участия всех заинтересованных сторон, каковыми в США являются фактически не только все государственные структуры, промышленность, частный капитал, но и рядовые граждане, военное ведомство в буквальном смысле пошло в народ, активно пропагандируя свое видение общенациональной проблемы №1. Одним из примеров такого новаторского подхода является программа DIAP (Defense Information Assurance Program), в рамках которой с участием таких ведущих фирм как Lucent Technologies, IBM, Microsoft, Intel, Cisco, Entrust, HP, Sun, GTE, Bay Networks, Axent, Network Associates, Motorola закладывается фундамент информационной безопасности не только военной инфраструктуры, но и всего американского общества в целом на ближайшие 10 лет.

В соответствии с секретной директивой Пентагона S-3600.1 *гарантия информации* определяется как "информационная операция или операции, связанные с защитой информации и информационных систем за счет обеспечения их готовности (доступности), целостности, аутентичности, конфиденциальности и непротиворечивости. Данные операции включают в себя восстановление информационных систем за счет объединения возможностей защиты, обнаружения и реагирования. При этом информация не будет раскрыта лицам, процессам или устройствам, не имеющим к ней прав доступа, будет обеспечена полная достоверность факта передачи, наличия самого сообщения и его отправителя, а также проверка прав на получение отдельных категорий информации, данные остаются в исходном виде и не могут быть случайно или преднамеренно изменены или уничтожены, будет обеспечен своевременный и надежный (по требованию) доступ к данным и информационным службам установленных пользователей, а отправитель данных получит уведомление факта доставки, также как получатель - подтверждение личности отправителя, и таким образом никто не сможет отрицать своего участия в обработке данных"[[7]](#footnote-7).

Тем самым классическое понятие информационной безопасности (INFOSEC - information security) как состояние информационных ресурсов было расширено и дополнено гарантированием их надлежащего использования даже в том случае, если эти ресурсы будут подвергнуты деструктивному воздействию как извне, так и изнутри. Иными словами в политике информационной безопасности четко обозначился сдвиг в сторону активных организационно-технических мероприятий защиты информационных ресурсов. Похоже, что американцы взяли за основу пропаганды знаний в области информационной безопасности советскую систему гражданской обороны  60-х, 70-х годов, когда население учили не только тому как надевать индивидуальные средства защиты и укрываться в бомбоубежищах, но и как вести радиационный, химический и бактериологический контроль и восстанавливать объекты народного хозяйства после применения оружия массового поражения.

Заметим, что это не единственное нововведение Пентагона в лексиконе информационных технологий, которое стало достоянием общественности не смотря на гриф секретности первоисточника. К числу таковых можно отнести следующие: "информационное противоборство", "информационное превосходство", "информационные операции (общие и специальные)", "информационная среда", "атака на компьютерные сети", "вторжение в информационные системы" и др. С некоторых пор американское военное ведомство считает полезным публиковать отдельные несекретные фрагменты из своих засекреченных официальных нормативных документов (директив, инструкций, меморандумов, уставов и наставлений), повышая информированность общества о потенциальных угрозах национальной безопасности. Военные терпеливо и настойчиво приучают все слои населения к своей терминологии, постепенно стирая грань между государством и обществом, обороной и производством, разведкой и предпринимательством, учебой и досугом[[8]](#footnote-8).

Профессиональная подготовка персонала в соответствии с новыми требованиями в области информационной безопасности является ключевым направлением реализации программы DIAP, в рамках которой на учебный процесс выделяется в общей сложности около 80 млн. $ на период до 2005 г.. При этом предполагается открыть специализированные курсы дистанционного обучения (свыше 20) в так называемом "виртуальном университете информационной безопасности" на базе сайтов в Интернете, в которых будут обучаться основам "стратегии глубокой эшелонированной защиты информационных ресурсов" администраторы (2 недели) и специалисты (3-5 дней) практически из всех федеральных ведомств, включая ЦРУ, ФБР, НАСА, Минфина, Минюста, Минэнерго и др. Ожидается, что за 5 лет будет подготовлено в общей сложности не менее 100 тыс. дипломированных специалистов в области информационной безопасности, готовых к любым неожиданностям в киберпространстве.

В каждом штате на период чрезвычайных условий (землетрясений, ураганов, наводнений, катастроф, террористических актов) создаются так называемые резервные центры обработки информации, в которых периодически собирается, накапливается и обновляется наиболее важная информация, необходимая для организации управления всех жизненно важных служб (полиции, скорой помощи, пожарной охраны и др.) в случае выхода из строя основных центров обработки информации и телекоммуникационных систем. Как правило такие центры оснащаются автономными источниками энергоснабжения (дизель - генераторами), способными поддерживать нормальный режим функционирования резервных информационных центров в течение нескольких суток до восстановления стационарной системы энергоснабжения. В повседневных условиях работу таких центров обеспечивает ограниченный по численности технический персонал, имеющий все необходимые навыки для организации работы центра в чрезвычайных условиях[[9]](#footnote-9).

Краткий обзор только некоторых наиболее важных и дорогостоящих программ развития информационных технологий в США на примере Пентагона показывает, что проблема информационной безопасности отдельно взятого ведомства по своему масштабу уже давно является общенациональной и для своего решения требует пересмотра устоявшихся подходов, принятия единых стандартов как в промышленности, так и в бизнесе, создания национальной системы подготовки специалистов соответствующего профиля, широкого информирования населения об угрозах и мерах по их предотвращению.

**Заключение**

По ряду экспертных оценок, изменение акцента в американской внешней политике на проблемы борьбы с терроризмом, уменьшило внешнеполитическое давление на Китай, открыв новые возможности по усилению его позиций не только в регионе, но и во всем мире. Отвечая на изменение военно-политической ситуации в мире, военно-политическое руководство КНР, по мнению рядя экспертов, ускорило темпы проведения реформы и модернизации вооруженных сил, направленных на скорейшее решение тайваньской проблемы.

В то же время целый ряд действий американских вооруженных сил, предпринятых в последнее время (вторжение в Афганистан, размещение вооруженных сил США в Средней Азии, углубление отношений в области военного сотрудничества между США с одной стороны и Пакистаном, Индией и Японией, с другой), привели к осознанию руководством Китая того факта, что основная цель проводимой США кампании состоит в скорейшем окружении Китая, обеспечения возможности его блокады и изоляции от внешнего мира[[10]](#footnote-10).

Как отмечается в ряде прогнозных исследований, выполненных за последние годы в аналитических центрах США, Китай становится главным экономическим и военным конкурентом Соединенных Штатов в наступившем столетии. Однако, несмотря на наличие такого серьезного противника, американское понимание стратегического наследия Китая, его Великой стратегии и роли информационной войны в поддержке этой стратегии, по мнению американских экспертов, серьезно недооценены. Существующий сегодня в США уровень развития приемов и методов анализа и прогнозирования не позволяет полностью постичь то сильное и глубокое воздействие, которое восточное стратегическое наследие имеет в действиях Китая.

Вместе с тем, как подчеркивают эксперты, несмотря на то, что за последние годы Китай добился существенного роста военного потенциала за счет поставок в войска новых систем вооружения, совершенствования боевой подготовки войск и изменения основных положений военной стратегии, в настоящее время Китай не имеет достаточно возможностей для проецирования необходимой военной силы вне национальных границ, что не позволяет говорить о возможности силового решения тайваньской проблемы в ближайшие годы[[11]](#footnote-11).

Таким образом, полагают американские военные эксперты, фокус краткосрочных и среднесрочных мероприятий по трансформации сил общего назначения НОАК будет сосредоточен на активной подготовке к возможной эскалации напряженности в Тайваньском проливе с учетом возможного вмешательства в конфликт и Соединенных Штатов. При этом в качестве целей ставится на только завоевание превосходства над вооруженными силами Тайваня, но и склонение США к скорейшему выходу из конфликта путем нанесения существенных потерь. Основной акцент при этом будет сделан на развитии ассиметричных методов вооруженной борьбы.

Эксперты особо отмечают, что отсутствие баланса между глобальными интересами Пекина и его низкой способностью проецировать силу для защиты своих интересов, как в региональном, так и глобальном масштабах создает ощущение уязвимости для самого Китая, что в свою очередь продолжает создавать напряженность между Китаем и Соединенными Штатами[[12]](#footnote-12).

**Список литературы**

* 1. Авинова Н.Н. Исторические аспекты информационных войн. – М, 2005. – 276 с.
	2. Социально-экономическая география мира/Под ред. В. В. Вольского. – М.: КРОН-ПРЕСС, 2007. – 592 с.
	3. Страны мира 2007: Справочник//под ред. Лаврова С.Б. – М.: Республика, 2008. – 532 с.
	4. Шакиров А. Р. Экономика США в 2007 г. // Мировая экономика и международные отношения. – 2008. – №1.
	5. Шацкий М.Ю. Мировые информационные войны и конфликты. – М, 2007. – 432 с.
	6. Щеголев Б.Н. США: экономическое развитие и проблемы внешней торговли. – М, 2006. – 138 с.
	7. Юриш И.Р. Экономические системы мира. – М, 2006. – 445 с.
	8. Ярунов И.И. Информация как мировая ценность. – М, 2006. – 177 с.
	9. www.allchina.ru
	10. www.osp.ru
1. Авинова Н.Н. Исторические аспекты информационных войн. – М, 2005. – 276 с. [↑](#footnote-ref-1)
2. www.allchina.ru [↑](#footnote-ref-2)
3. Социально-экономическая география мира/Под ред. В. В. Вольского. – М.: КРОН-ПРЕСС, 2007. – 592 с. [↑](#footnote-ref-3)
4. www.allchina.ru [↑](#footnote-ref-4)
5. Страны мира 2007: Справочник//под ред. Лаврова С.Б. – М.: Республика, 2008. – 532 с. [↑](#footnote-ref-5)
6. Щеголев Б.Н. США: экономическое развитие и проблемы внешней торговли. – М, 2006. – 138 с. [↑](#footnote-ref-6)
7. www.osp.ru [↑](#footnote-ref-7)
8. Щеголев Б.Н. США: экономическое развитие и проблемы внешней торговли. – М, 2006. – 138 с. [↑](#footnote-ref-8)
9. Ярунов И.И. Информация как мировая ценность. – М, 2006. – 177 с. [↑](#footnote-ref-9)
10. Авинова Н.Н. Исторические аспекты информационных войн. – М, 2005. – 276 с. [↑](#footnote-ref-10)
11. Социально-экономическая география мира/Под ред. В. В. Вольского. – М.: КРОН-ПРЕСС, 2007. – 592 с. [↑](#footnote-ref-11)
12. www.osp.ru [↑](#footnote-ref-12)