

ДИПЛОМАТИЧЕСКАЯ АКАДЕМИЯ
МИНИСТЕРСТВА ИНОСТРАННЫХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

На правах рукописи



003 176 107

ДЕНЬЩИКОВ Александр Леонидович

**ИНФОРМАЦИОННАЯ СТРАТЕГИЯ США
(АНАЛИЗ, СОВРЕМЕННОСТЬ, ПЕРСПЕКТИВЫ)**

Специальность 23 00 02 – политические институты,
этнополитическая конфликтология,
национальные и политические
процессы и технологии

15 НОЯ 2007

**АВТОРЕФРАТ
диссертации на соискание ученой степени
кандидата политических наук**

**Москва
2007**

Работа выполнена на кафедре Дипломатии Дипломатической академии МИД России

Научный руководитель:

Панарин Игорь Николаевич -
доктор политических наук, профессор, декан в/о факультета
"Международные отношения" Дипломатической академии
МИД РФ

Официальные оппоненты:

Фролов Дмитрий Борисович -
доктор политических наук, первый заместитель начальника
управления Центра информационной безопасности ФСБ
РФ

Развин Петр Александрович -
кандидат политических наук, начальник отдела
международных обменов Управления научно –
координационной работы и международных связей
Дипломатической академии МИД РФ

Ведущая организация:

Академия Генерального штаба МО РФ

Защита состоится " " 2007 г в часов на заседании
диссертационного совета Д 290 001.01 в Дипломатической академии МИД России
по адресу 107078, Москва, Большой Козловский переулок, д 4

С диссертацией можно ознакомиться в библиотеке Дипломатической академии
МИД России

Автореферат разослан «18» октября 2007г

Ученый секретарь
диссертационного совета
кандидат политических
наук



А.Е. Тарасов

I. ОБЩАЯ ХАРАКТЕРИСТИКА ДИССЕРТАЦИИ

Широкая информатизация в современных условиях создала в различных государствах и их вооруженных силах качественно новую ситуацию. Наглядной иллюстрацией ее практического проявления служат вооруженные конфликты и локальные войны последних десятилетий XX века. Их анализ со всей очевидностью свидетельствует о том, что ход и исход нынешних и будущих боевых действий, причем любого масштаба, во многом определяются искусством ведения информационного противоборства (ИП).

Последние два десятилетия ушедшего века отмечены глобальной борьбой США за общественное сознание народов всей планеты на основе координации деятельности всех государственных и коммерческих структур, с масштабным использованием новейших информационных технологий. Следует отметить, что резкому нарастанию количественных и качественных характеристик информационного противоборства сопутствовало развитие единого мирового информационного пространства.

Сегодня между ведущими государствами развернулось геостратегическое информационное противоборство за достижение превосходства в мировом информационном пространстве. Безусловно, что особо важную роль оно стало играть в сфере военной безопасности. В настоящее время наиболее развитые страны располагают мощным информационным потенциалом, который в определенных условиях обеспечивает достижение ими самых различных политических целей. Острота и непредсказуемость информационного противоборства подпитываются тем обстоятельством, что до сей поры нет разработанных международных юридических норм его ведения.

В современном мире сложилась глобальная система идейно-политической и военно-экономической гегемонии США. За ними после развала СССР в мире закрепился статус первой и единственной сверхдержавы. Они лидируют в процессе информационной революции. Здесь новые информационные системы и технологии уже стали неотъемлемой частью не только жизни общества, но и отдельных граждан. Прежде всего это касается электронных средств массовой информации, интернета, различного рода телекоммуникационных систем (имеются в виду мобильная связь, глобальная высокоточная навигация, оптико-волоконные и беспроводные сети передачи данных), используемых в профессиональной деятельности и в быту. Словом, информационная эра стала оказывать и прямое, и косвенное воздействие на все стороны жизнедеятельности человека.

События второй половины XX века показали, что новые технологии еще больше увеличили потенциальные возможности информации в войне, а также

подтвердили важность ее роли в обеспечении не только национальной и военной безопасности отдельной страны, но и международной безопасности в целом. Однако именно эти достижения привели к тому, что открылись новые угрозы безопасности государств.

Дело в том, что прозрачность государственных границ для информационных потоков создала принципиально иную ситуацию в функционировании институтов государственной власти, а интеграция инфраструктур государства на основе информационных систем (банковско-финансовой, транспортной, электрических сетей, нефте- и газопроводов) сделала их потенциальными объектами средств информационного противоборства. Более того, стало очевидным, что фактическая неуправляемость информационным пространством собственной страны приводит к значительному ограничению ее суверенитета, а то и даже ставит под вопрос возможность дальнейшего существования государства в его классической форме.

В США новые взгляды на информационную стратегию прошли этап первоначального осмысления, оплодотворив процесс стратегического (геостратегического) планирования до 2020г, разработки документов, соответствующих следующим элементам структурно-логической схемы программы, бюджетные предложения, оперативные планы, организационно-методические разработки.

Актуальность диссертационного исследования обусловливается следующими обстоятельствами

- особой ролью США в информационно-психологическом противоборстве как явлении современной политической действительности и как особой формы идеологической борьбы как в мирное, так и в военное время,

- информационное противоборство стало реальной силой для достижения поставленных целей в различных сферах жизнедеятельности государства и общества. Практическая реализация целей и задач информационного противоборства в зарубежных странах подчеркивает необходимость скорейшей военно-научной проработки различных аспектов отечественной теории информационного противоборства, на основании которой можно будет осуществлять практические действия в интересах национальной и военной безопасности России,

- необходимостью научного анализа форм и методов информационно-психологического воздействия, защиты населения и личного состава войск от негативных воздействий как в военное, так и в мирное время, используемых США, что позволит критически оценить американский опыт в построении информационной стратегии, целиком рассмотреть ее систему, определить

координатора решения вопросов в этой области, роль и полномочия различных ведомств с учетом специфики их деятельности. Изучение теории и практики информационных операций, проводимых США, абсолютно необходимо для анализа вероятных угроз Российской Федерации,

- потребностью в уточнении и разработке практических рекомендаций по защите от информационно-психологических воздействий органам государственной власти и управления Российской Федерации в интересах повышения эффективности информационной политики, обеспечения информационной безопасности личности, общества и государства

Степень научной разработанности проблемы.

Отечественную литературу по вопросам информационного противоборства можно разделить на несколько групп

К первой группе следует отнести руководящие документы, регламентирующие деятельность высших органов государственной власти и управления в области информационной политики¹. В них изложены концептуальные основы и целевые установки, однако в прямой постановке проблемы информационно-психологической безопасности практически не раскрыты, к тому же отсутствует анализ возможных последствий использования методов ИП против населения и войск

Вторую группу источников составляют фундаментальные исследования отечественных ученых по общим проблемам теории безопасности и национальной безопасности Российской Федерации. Баршполец В., Возжеников А В., Дзлиев М И., Золотарев В А., Косолапов Н., Ладыгин Ф., Лузинян В., Пионтковский А А., Прохожев А А., Ромашкин П., Смутьский С В., Турко Н И., Урсул А Д., Цыганков П А., Цыгичко В Н., Чебан В В. и др.², имеющие общеметодологический характер

Особое место здесь занимают труды, в которых теоретико-методологические обобщения развиты и конкретизированы применительно к

¹ Конституция Российской Федерации – М., 1994, Военная доктрина Российской Федерации – М., 2000, Концепция национальной безопасности Российской Федерации – М., 2000, Концепция внешней политики Российской Федерации – М., 2000, Доктрина информационной безопасности Российской Федерации //Российская газета – 2000 - № 187 – 28 сентября

² Баршполец В. Политическая безопасность России //Вестн воен информ / «Военинформ» и РИА «Новости» – 1998 - № 12, Возжеников А В. Национальная безопасность России: методология комплексного исследования и политика обеспечения – М. Изд-во РАГС, 2002, Дзлиев М И., Урсул А Д. Основы обеспечения безопасности России – М. Изд-во «Экономика», 2003, Косолапов Н. Сила, насилие, безопасность: современная диалектика взаимосвязей //Мировая экономика и международные отношения – 1992 - № 11, Ладыгин Ф. О характере современных внешних угроз и вызовов национальным интересам и безопасности России //Ядерный контроль/ ПИР-Центр – 1999 - № 6, Лузинян В. Методология исследования проблем безопасности и стабильности //Военная мысль – 1993 - № 3, Общая теория национальной безопасности. Учебник. Под общ. ред. А А Прохорова – М. Изд-во РАГС, 2005, Цыганков П А. Безопасность: кооперативная или корпоративная (Критический анализ международно-политической концепции) //Политические исследования – 2000 - № 3, Цыгичко В Н., Пионтковский А А. Возможные вызовы национальной безопасности России в начале XXI века //Военная мысль – 2001 - № 2 и др.

проблемам информационной безопасности Андреев Э М, Василенко И А, Корнеев И К, Крутских А, Поздняков А И, Степанов Е А, Турко Н И, Шевченко А В, Ярочкин В И³ и военной безопасности Барынькин В М, Булгаков В, Велесов С Л, Громов Б В, Дмитриев А П, Золотарев В А, Лутовинов В Н, Манилов В А, Панарин И Н, Рогов С М, Серебрянников В В и др⁴

В некоторые из этих работ рассматриваются и различные аспекты информационно-психологической безопасности, содержится характеристика информационного противоборства

Третья группа работ непосредственно включает научные труды по проблемам информационной политики, информационного противоборства и информационно-психологической борьбы Борисенко М В, Вепринцев В Б, Винокуров И Н, Володенков С В, Волковский Н Л, Грачев Г В, Грешневиков А, Гриняев С Н, Забарин А В, Зимичев А М, Иванов О В, Кара-Мурза С Г, Караяни А Г, Комов С А, Костин Н А, Крысько В Г, Лисичкин В А, Манойло А В, Мельник И К, Модестов С А, Мухин А А, Назаретян А П, Некляев С Э, Ососков В П, Павлова Е К, Панарин И Н, Петренко А И, Попов В Д, Поченцов Г Г, Пригожин А И, Прокофьев В Ф, Расторгуев С П, Тавокин Е П, Фролов Д Б, Шелепин Л А, Цуладзе А, Цымбал В И, Яковлев И Г и др⁵ Данные работы содержат анализ чрезвычайно широкого спектра вопросов

³ Андреев Э М, Миронов А В Социальные проблемы интеллектуальной уязвимости и информационной безопасности //Социально-гуманитарные знания – 2000 - № 4, Василенко И А Информационные ресурсы власти и формирование новой постклассической картины политического мира XXI в //Вестник МГУ Серия 12 – 2004 - № 2, Поздняков А И Информационная безопасность страны и вооруженные силы: сущность, структура, актуальные проблемы обеспечения //Национальная безопасность: актуальные проблемы – М ВАГШ, 2000, Крутских А Информационный вызов безопасности на рубеже XXI века //Международная жизнь – 1999 - № 2, Шевченко А В Информационная устойчивость политической системы – М РАГС, 2004, Ярочкин В И Информационная безопасность – М, 2000 и др

⁴ Булгаков В Вооруженный конфликт: формы и способы действий войск //Военная мысль – 2002 - № 1, Золотарев В А Военная безопасность Отечества (историко-правовое исследование) 2-е изд. – М «КАНОН-пресс» – «Кучково поле», 1998, Лутовинов В, Орлов С Концепция национальной безопасности, Военная доктрина Российской Федерации об основных угрозах военной безопасности страны //Ориентир – 2000 - № 10, Манилов В А Безопасность в эпоху партнерства – М ТЕРРА, 1999, Панарин И Н Информационная война и Россия 2001 Проскурин С Военная сила и постиндустриальное общество //Мировая экономика и международные отношения – 1996 - № 10, Турко Н И Силовое сдерживание в системе обеспечения безопасности государства – М ВАГШ, 2000, Чебан В В Геополитическое положение и военная безопасность России – М Фонд «Воин», ИВНЦ «Отчество и воин», 1997 и др

⁵ Вепринцев В Б, Манойло А В, Петренко А И, Фролов Д Б Операции информационно-психологической войны: методы, средства, технологии, краткий энциклопедический словарь – М Горячая линия – Телеком, 2003, Грачев Г В, Мельник И К Манипулирование личностью: Организация, способы и технологии и информационно-технологического содействия – М, 2004, Кара-Мурза С Г Манипуляция сознанием – М Алгоритм, 2000, Караяни А Г Информационно-психологическое противоборство в современной войне – М ВУ, 1997, Крысько В Секреты психологической войны (цели, задачи, методы, формы, опыт) – Минск, 1999, Панарин И Н Информационная война и Россия – М Изд дом Мир безопасности, 2000, Он же Информационная война и власть – М Мир безопасности, 2001, Поченцов Г Г Информационные войны – М Рефл-Бук, К Ваклер, 2000, Он же Пропаганда и контрпропаганда – М Центр, 2004, Расторгуев С П Информационная война – М Радио и связь, 1998, Цуладзе А Политические манипуляции или покорение толпы – М, 1999, Toffler A The Third Wave – N Y, 1980 и др

противоборства в информационной сфере, в т ч и некоторые аспекты содержания и технологий применения ИП в политических целях

Основу зарубежной источниковой базы составляют различные исторические документы, а также объединенные доктрины, полевые уставы и директивы министерства обороны США, регламентирующие деятельность системы информационных операций. Вся данную базу можно разделить на несколько групп.

Первая группа – это открытые документы администрации президента США, конгресса и соответствующих правительственных ведомств Соединенных Штатов, в которых рассматриваются вопросы, касающиеся информационных операций, информационного обеспечения, защиты важной государственной инфраструктуры. К ним в первую очередь относятся «Доклад Президентской комиссии по защите критической инфраструктуры», «Президентская директива по защите критической инфраструктуры», президентский доклад «Стратегия национальной безопасности в новом веке», «Национальный план защиты информационных систем», «Отчет президента США о действиях по защите критической инфраструктуры» и др.⁶

Вторая группа – это руководящие и доктринальные⁷ документы министерства обороны США, Комитета начальников штабов, министерств и штабов видов вооруженных сил, в той или иной степени касающиеся различных аспектов информационного противоборства. Это прежде всего «Объединенная перспектива 2010», «Концепция будущих объединенных операций расширенная объединенная перспектива 2010», «Объединенная перспектива 2020», ежегодные доклады министра обороны США Президенту и Конгрессу, «Четырехлетние оборонные обзоры», «Объединенная доктрина информационных операций», «Объединенная доктрина борьбы с системами управления», полевой устав FM-106 «Информационные операции», устав ВВС AFD 2-5 «Информационные операции», полевой устав FM-3-0 «Операции» и др.⁸

⁶ The President's Commission on Critical Infrastructure Protection. Summary Edition of Critical Foundations. Thinking Differently. Washington. October 1997, Presidential Decision Directive 63. The Clinton Administration's Policy on Critical Infrastructure Protection. Washington. May 1998, A national security strategy for a new century. Washington. December 1999, National Plan for Information Systems Protection. Version 1.0. An Invitation to a Dialogue. Washington. 2000, Report of the President of the United States of Federal Critical Infrastructure Protection Activities. Washington. January 2001 и др.

⁷ Под доктриной в Соединенных Штатах подразумевают фундаментальные принципы, направляющие действия военной силы или ее элементов в поддержку национальных целей. Под «объединенными доктринами» (joint doctrine) понимаются фундаментальные принципы, регулирующие использование двух или более видов вооруженных сил в скоординированной деятельности для достижения общей цели.

⁸ Joint Vision 2010. Washington. 1995, Concept for Future Joint Operations. Expanding Joint Vision 2010. Ft Monroe 1997, Information Warfare. A Strategy for Peace and the Decisive Edge in War. Washington. 1996, Joint Vision 2020. Washington. 2000, Annual Report to the President and Congress. Washington. January 2001, Quadrennial Defense Review. Washington. 30 September 2001, Transforming Defense. National Security in the 21st Century. Arlington. December 1997, Joint Doctrine for Information Operations. Washington. 9 October 1998, Joint Doctrine for Command

Третья группа – это основополагающие научные труды американских авторов по различным аспектам исследуемой темы Среди них особо стоит выделить работы следующих авторов Тоффлер О – «Третья волна», «Перераспределение власти», «Война и антивойна выживание в XXI веке»; Агуилла Д и Ронфельд Д – «Кибервойна приближается», «Информация, власть и великая стратегия», Альбертс Д – «Оборонная информационная борьба», Штейн Дж – «Информационная борьба», Шафрански Р – «Теория информационной войны подготовка 2020», Швартау В – «Информационная борьба хаос на информационной автостраде», Либики М – «Что такое информационная война», Томас Т – «Российские взгляды на борьбу на основе информации» и др.⁹

Четвертая группа – это разработки американских научно-исследовательских центров и военно-учебных заведений, а также западноевропейские и китайские исследования по проблеме информационного противоборства В первую очередь это ряд отчетов корпорации РЭНД, сделанных по заказу министерства обороны США «В лагере Афины подготовка к конфликтам в информационном веке», «Появление неополитики к американской информационной стратегии», «Стратегическая информационная борьба новое лицо войны», «Усиливающаяся стратегическая информационная борьба», «Появление сетевых войн», «На следующий день в киберпространстве», «Глобальная технологическая революция» и другие, а также разработки Национального университета обороны, Института оборонного анализа, Центра международных и стратегических исследований, различных научно-исследовательских групп, занимающихся исследованием тех или иных аспектов информационного противоборства и использования информации¹⁰

and Control Warfare (C2W) Washington, 7 February 1996, Field Manual FM 100-6 Information Operations Washington August, 1996, Information Operations Air Force Doctrine Documents 2-5 Alabama 5 August 1998, Information Warfare Legal, Regulatory, Policy and Organizational Considerations for Assurance Washington 1996 и др

⁹ Toffler A The Thrd Wave New York 1980, Toffler O War and Anti-War Survival at the Dawn of the 21st Century Boston 1993, Arquilla J, Ronfeldt D "Cyberwar Is Coming!" Comparative Strategy Vol 12, N 2, Summer 1993, Szafranski R A Theory of Information Warfare Preparing for 2020 Airpower Journal Spring 1995, Libicki M What is Information Warfare? Washington 1995, Libicki M Protecting the United States in Cyberspace Washington 1996, Campen A The First Information War Fairfax 1992, Schwartau W Information Warfare Airpower Journal Spring 1995, Thomas T Russian Views on Information-Based Warfare Airpower Journal Special Edition 1996 и др

¹⁰ Molander R and others Strategic is Information Warfare A New Face of War RAND 1996, Molander R Strategic is Information Warfare Rising RAND 1998, Arquilla J, Ronfeldt D, (eds) In Athena's Camp Preparing for Conflict in the Information Age RAND 1997, Arquilla J, Ronfeldt D The Emergence of Noopolitik Toward an American Information Strategy RAND 1997, The Global Course of the Information Revolution Political, Economic, and Social Consequences RAND 2000, Wilson P, Mussington D, Mesic R, Anderson R, Hearn A An Exploration of Cyberspace security R & D Investment strategies for DARPA "The Day After in Cyberspace II" RAND 1996, The global technology revolution bio/nano/materials trends and their synergies with information technology by 2015 RAND 2001, Information Warfare Selected Long-Range Technology Applications IDA 1996, Information Warfare Technologies Survey of Selected Civil Sector Activities IDA 1996, Global Trends 2015 A Dialogue About the Future With Nongovernment Experts NIC December 2000 и др

Несмотря на то, что проблемы информационного противоборства разрабатываются уже достаточно длительный период, особую значимость они приобретают именно сегодня, когда роль США в данной сфере значительно возросла. Поэтому, отдавая должное теоретической глубине, обстоятельности, разносторонности научных исследований и признавая вклад всех вышеуказанных, а также других авторов в развитие теоретико-методологических основ теории информационного противоборства, следует отметить, что особенности информационных воздействий США в современном информационном противоборстве исследованы не в полной мере.

Теоретико-методологической основой исследования явился структурный, системный и сравнительный анализ, который сделал возможным изучение объекта и предмета исследования в комплексе, выявление их наиболее существенных элементов, а также взаимозависимости и взаимообусловленности между ними.

Предметом исследования является роль и место информационного противоборства во внешней и внутренней политике США.

Объектом исследования является механизм ведения информационного противоборства США.

Положения, выносимые на защиту:

- выводы, сделанные на основе исследования теории и практики информационных операций вооруженных сил США,
- результаты исследования структуры, содержания, форм и методов ведения информационного противоборства США,
- определение сущности информационного противоборства, его места и роли в межгосударственном вооруженном противоборстве. Итоговые данные о практической роли и значении информационного противоборства, осуществляемого США,
- рекомендации и предложения, вытекающие из результатов исследования структуры, содержания и методов ведения информационного противоборства вооруженными силами США.

Основной целью исследования является комплексный анализ и классификация основных направлений информационной стратегии США по созданию и использованию средств ведения информационного противоборства в различных сферах.

Достижение поставленной цели мыслится как решение следующих задач:

- провести комплексный анализ взглядов военно-политического руководства США на механизм ведения информационного противоборства в конце XX-начале XXI веков,

- провести анализ основных направлений ведения информационного противоборства США,
- оценить роль США в ведении информационного противоборства и показать перспективы развития концепции информационного противоборства,
- выявить новые элементы в информационной стратегии США,
- проанализировать основные аспекты плана защиты информационной системы США

Научная новизна исследования состоит в следующем

- на основе всестороннего изучения значительного объема зарубежных и отечественных источников проведен комплексный анализ взглядов военно-политического руководства США на механизм ведения информационного противоборства в конце XX-начале XXI веков. Обобщен новый материал, в научный оборот введены источники, которые ранее по объективным причинам не могли быть использованы в отечественной научной и специальной литературе,
- исследованы содержание, аппарат, формы и методы реализации задач информационного противоборства, их роль и место в общей системе применения вооруженных сил США,
- уточнено понимание ряда терминов информационного противоборства США, рассмотрены принципы его практического осуществления,
- сформулированы выводы, научно-практические рекомендации и предложения, вытекающие из анализа структуры аппарата, форм, методов и содержания информационных операций, проводимых вооруженными силами США
- определена сущность и структура стратегической информационной войны, рассмотрена ее роль как явления современной политической действительности и значение в системе противоборства государств

Практическая значимость работы заключается в том, что ее положения и выводы могут быть использованы в практической деятельности МИД России, других государственных министерств и ведомств, а также в сфере научных исследований и применительно к учебному процессу в Дипломатической академии, МГИМО(Университет) МИД России и других вузах соответствующего профиля

Структура диссертации обусловлена целями, общим замыслом и логикой работы. Диссертация состоит из введения, трех глав, заключения и списка литературы

II. ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** обосновывается актуальность выбранной темы, раскрывается степень ее разработанности, определяется предмет, объект, цели и задачи исследования, показаны научная новизна и степень значимости

В первой главе – **“Основные направления ведения информационного противоборства”** представлена и обоснована классификация основных направлений ИП. Рассматриваются основные группы целей на которые предполагается оказывать целенаправленное информационное воздействие в ходе ведения ИП

Специфические черты информационного противоборства вызывают настоятельную потребность в изучении и обобщении его содержания с целью выработки новых положений как военной теории, так и теории информационной безопасности государства

По замыслу американских разработчиков, информационное противоборство, реализуемое через информационные операции, подразумевает использование сил и средств информационной борьбы для подготовки и применения вооруженных сил США и включает в себя деятельность высшего военно-политического руководства, органов государственного и военного управления, средств массовой информации, соответствующих компонентов информационного противоборства, направленную на подготовку и применение вооруженных сил США, формирование благоприятной информационной среды и создание условий для выполнения поставленных перед ними задач

В ходе исследования было изучено два направления в информационном противоборстве: информационно-психологическое и информационно-техническое. При информационно-психологическом противоборстве главными объектами воздействия, а, следовательно, и защиты являются психика военно-политического руководства, личного состава вооруженных сил, спецслужб и населения, а также системы формирования общественного мнения и принятия решений. При информационно-техническом противоборстве главными объектами воздействия и защиты являются информационно-технические системы (системы связи, телекоммуникационные и компьютерные системы, радиоэлектронные средства и т.д.)

В США для описания информационного противоборства чаще всего используются такие термины, как «информационные операции» (ИО) («Information operations»), «информационная борьба» («Information warfare»)

По взглядам американского военного руководства, информационные операции в ходе ведения военных действий представляют собой совокупностью методов воздействия на информационные ресурсы и системы противника при защите собственных информационных ресурсов и систем в целях захвата информационного превосходства, доминирования в информационном пространстве. Таким образом, понятие «информационная борьба» («Information warfare»), по взглядам американского военного руководства, включает в себя комплексное применение сил и средств информационных операций и вооруженной борьбы в угрожаемый период и при ведении боевых действий.

В США новые взгляды на информационную стратегию прошли этап первоначального осмысления, оплодотворив процесс стратегического (геостратегического) планирования до 2020г, разработки документов, соответствующих следующим элементам структурно-логической схемы программы, бюджетные предложения, оперативные планы, организационно-методические разработки.

К числу первых официальных документов Пентагона по этой проблеме можно отнести директиву МО США Т 3600 1 от 21 декабря 1992 года под названием "Информационная война". В 1993 году в директиве Комитета начальников штабов № 30 уже были изложены основные принципы ведения информационной войны.

Начиная с 1994 года, в США проводятся официальные научные конференции по "информационной войне" с участием видных представителей военно-политического руководства страны.

В августе 1995 года национальный Институт Обороны США публикует работу Мартина Либки "Что такое информационная война?". В ней автор определил семь форм информационной войны.

В конце 1998 года Комитет начальников штабов ВС США издал документ "Доктрина проведения информационных операций" (Joint doctrine of information operations).

В нем впервые официально подтверждается факт подготовки американцев к проведению наступательных информационных операций. Ранее представители Пентагона всегда подчеркивали оборонительную направленность мероприятий США в информационной сфере.

Новым документом предусматривается возможность проведения наступательных информационных операций не только в военное, но и мирное время. При этом представители США, комментируя эти положения, утверждают, что использование наступательного информационного оружия будет проводиться при полном соблюдении соответствующих международных норм и договоров. Однако на сегодняшний день подобные международные

соглашения либо отсутствуют, либо находятся на ранних стадиях проработки. Предложения МИД России, Организации Объединенных Наций по правовому регулированию мировой информационной сферы встречают жесткое американское сопротивление.

Осенью 1999 года в США создан центр ведения кибернетической войны (наступательной и оборонительной).

Идея завоевания информационного превосходства над противником путем проведения информационных операций последовательно воплощалась в документах КНШ МО США "Единые перспективы 2010" и "Единые перспективы 2020", а также в документах МО США "Четырехлетний обзор состояния вооруженных сил" от 2001 и 2006 годов. В них определены цели, задачи и основные принципы информационной борьбы, обязанности руководящих органов и должностных лиц по ее организации и планированию в мирное время и в кризисной обстановке.

К концу 90-х годов в США сформировался целый ряд экспертно-аналитических групп, принадлежащих к различным теоретическим школам и исследующих различные аспекты многофакторной проблемы ведения информационного противоборства. Уже в настоящее время результаты проводимых этими группами разработок в значительной степени влияют на выработку конкретных практических шагов в сфере ведения ИП, принимаемых на высшем военно-политическом и политическом уровне западных стран. В связи с этим представляется целесообразным рассмотреть основные теоретические предпосылки и тематику исследований, проводимых наиболее известными из этих экспертно-аналитических групп.

Далее автором рассматриваются концепции "кибернетической войны" и "сетевой войны", выдвинутые сотрудниками RAND Corporation Джоном Арквиллой и Дэвидом Ронфельдом, которые в настоящее время получили весьма широкое распространение. В частности, концепция "кибернетической войны" подразумевает, что в ходе будущих военных конфликтов информация будет играть решающую роль, а ключом к успеху будет являться достижение информационного превосходства.

"Сетевая война" является более сложной формой будущего военно-политического конфликта, в ходе которого борьба за информационное доминирование затронет социальные и национальные особенности сторон, вовлеченных в конфликт.

Затем диссертантом анализируются работы представителей теоретической группы Университета ВВС США (Air University, Maxwell Airforce Base, Alabama) Джорджа Стейна, Ричарда Шафрански и Оуэна Дженсена, которые полагают, что в будущем конфликте решающую роль будет

играть сама информация (точнее, знания), которая при этом будет являться одновременно и оружием, и целью, преследуемой конфликтом. Такой тип конфликта, по их представлениям, будет проходить в до неузнаваемости измененных условиях. Предполагается, что в ходе конфликта, принципиально отличающегося от традиционного, не будут задействованы не только традиционные системы вооружений, но и такие высокотехнологические системы, как "цифровое поле боя" и т.п., обычно ассоциируемые с ведением ИП. Иначе говоря, новые информационные технологии позволят "сражаться" непосредственно с сознанием противника, активно используя информационные сети и различные СМИ для ведения адаптированной пропаганды и создания у противника искаженной картины мира. Сами информационные технологии рассматриваются в данной концепции только как средство, облегчающее стратегическое информационное доминирование, под которым в данном случае понимается создание таких информационных условий, в которых действия противника в конечном итоге неизбежно окажутся выгодными или будут направлены на обслуживание интересов противоположной стороны. Как утверждают сторонники этой теоретической школы, ИП представляет собой своего рода функциональный эквивалент концепции использования воздушной силы для решения стратегических задач.

Автором рассмотрены и работы одного из наиболее влиятельных теоретиков в области ИП Мартина Либки (приложившего много усилий для того, чтобы теоретические разработки в этой области нашли свое практическое воплощение) который полагает, что в будущем информация станет основным средством сдерживания вооруженных конфликтов. По его мнению, взаимосвязанная информационная система, состоящая из сети космических спутников слежения, наземных, воздушных и морских датчиков, позволит контролировать любую военную активность на планете и, соответственно, позволит своевременно применять превентивные меры. В таких условиях любые действия потенциального агрессора будут абсолютно прозрачны для противоположной стороны и международного сообщества в целом. Соответственно, агрессор может быть лишен даже самой возможности проведения военных приготовлений, поскольку глобализация мировых информационных систем позволит парализовать и отрезать его экономические и информационные системы от прочего мира.

Для нас представляется важным то, что анализ появляющихся и постоянно уточняемых теоретических построений позволяет выявить общий вектор развития ИП. В частности, наиболее характерной чертой современных подходов является то, что основное внимание теперь, в отличие от предыдущих лет, уделяется уже не собственно технической (технологической) стороне

проблемы, а организационным и психологическим аспектам ИП, причем информация сама рассматривается как цель и средство действий, предпринимаемых для разрешения конфликта. Такая смена приоритетов, естественно, не снимает с повестки дня разработку и совершенствование технических аспектов, поскольку информационные технологии выступают если не первостепенными, то необходимыми компонентами даже в самых футуристических теориях ИП.

Детальный анализ проблемы ведения ИП, включая определение возможностей для планирования мероприятий по осуществлению или отражению ИО, требует более четкого выявления основных направлений ИП. Согласно Маргину Либики, можно выделить семь таких направлений, которые легли в основу нормативных документов военно-политического руководства США:

- 1 Борьба с системами управления (C2W – Command and Control Warfare),
- 2 Информационно-разведывательные операции (Intelligence-based operations),
- 3 Электронная борьба (EW),
- 4 Психологическая борьба (PSYOPS),
- 5 «Хакерская» борьба (Hackerwar),
- 6 «Кибернетическая» и «сетевая» борьба (Cyberwar combat in the virtual realm),
- 7 Экономическая информационная борьба

Диссертант отдает себе отчет в некоторой уязвимости для критики изложенной выше классификации. Однако выделение всех возможных оснований для классификации не являлось целью данного исследования, научная задача которого состояла в реализации комплексного подхода к классификации ИП. Эту попытку можно рассматривать в качестве основы для дальнейших исследований.

Во второй главе – “Стратегии информационного противоборства США” описаны методы информационного противоборства в военных операциях, рассмотрены возможности средств массовой информации в локальных вооруженных конфликтах, проанализированы взгляды военных экспертов США на ведение информационного противоборства.

Одним из основных направлений современной стратегии национальной безопасности США, и это эксплицитно закреплено в соответствующих доктринальных документах, на настоящее время является наращивание информационной мощи, главными составляющими которой считаются системы военной разведки, связи и управления. При этом такое наращивание будет проводиться в условиях, когда общую численность вооруженных сил США, в

соответствии с принципами новой американской оборонной политики (передовое присутствие, реагирование на кризисные ситуации, коллективная безопасность и др.), в рамках концепции «минимальных сил» предполагается сократить в начале XXI века примерно на 25%

Ключевым понятием, введенным в отчете MR-964-OSD, является классификация стратегического противоборства на первое и второе поколение. При этом стратегическое ИП первого поколения рассматривается наряду с традиционными средствами противоборства (ядерными, химическими, биологическими и другими). Подчеркивается, что оно больше ориентировано на дезорганизацию деятельности систем управления и проводится скорее как обеспечение действий традиционных сил и средств. Такое восприятие информационного противоборства свойственно начальному этапу осмысления проблемы. Стратегическое ИП первого поколения можно определить как «один из нескольких компонентов будущего стратегического противоборства, применяемый совместно с другими инструментами достижения цели». Таким образом, понятие «стратегическое информационное противоборства первого поколения» фактически вообрало в себя основные методы информационной войны, которые США реализуют в настоящее время на государственном и военном уровнях и от которых не намерены отказываться в обозримом будущем.

Дальнейшее изучение проблемы привело к введению понятия «стратегического информационного противоборства второго поколения» (2nd Generation Strategic Information Warfare). Это понятие можно определить как «принципиально новый тип стратегического противоборства, вызванный к жизни информационной революцией, вводящий в круг возможных сфер противоборства информационное пространство и ряд других областей (прежде всего экономику) и продолжающийся долгое время: недели, месяцы и годы». Отмечается, что развитие и совершенствование подходов к ведению стратегического ИП второго поколения в перспективе может привести к полному отказу от использования военной силы, поскольку скоординированные информационные акции могут позволить обойтись без этой крайней меры. Стоит заметить, что если последствия стратегического ИП первого поколения еще могут быть прогнозируемы с использованием существующих методик, то второе поколение противоборства на текущий момент весьма трудно формализуемо, и существующие методики прогноза могут быть применены к анализу последствий весьма условно.

Анализ опубликованных результатов военных исследований и других материалов открытой печати показывает, что в настоящее время специалисты Минобороны, разведывательного сообщества, других правительственных

ведомств и представители академических кругов США ведут усиленную проработку новых концепций и принципов строительства, управления, организации и применения вооруженных сил, которые должны прийти на смену присущей индустриальной эпохе модели массовой мобилизации, дислокации, оснащения и использования военной мощи

Среди предлагаемых новых концепций применения в ходе ведения войны высоких информационных технологий особое внимание обращает на себя концепция «информационного господства» ("Единые перспективы 2010" и "Единые перспективы 2020", а также в документах МО США "Четырехлетний обзор состояния вооруженных сил" от 2001 и 2006 годов)

В рамках этой концепции, предусматривающей широкое использование имеющегося перспективного технологического задела и методов моделирования под «информационным господством» понимается возможность «опережающего» получения необходимых сведений и данных о тактической или стратегической ситуации, позволяющих принимать своевременные решения (в соответствии с принципами американской концепции «кризисного управления») по нейтрализации и сдерживанию действий противоборствующей стороны. Отражением идей данной концепции является использование возможностей СМИ в локальных вооруженных конфликтах. Ведущие мировые державы благодаря наличию отлаженного механизма государственного контроля за проведением информационной политики располагают широкими и разнообразными возможностями для достижения своих политических целей и защиты государственных интересов посредством влияния через СМИ на общественное сознание как внутри своих стран, так и за рубежом. Данный вывод относится также к ситуациям, когда складываются предпосылки для принятия решения об участии вооруженных сил ведущих держав в локальных вооруженных конфликтах в различных регионах. При этом использование противоборствующими сторонами возможностей СМИ в своих интересах, как правило, становится составной частью общего сценария проведения операций с применением вооруженных сил. Наиболее наглядно это проявилось при подготовке операции "Буря в пустыне", в ходе вторжения войск США на Гаити (1994), боевых действий армии Израиля в Южном Ливане (1996), а также агрессии НАТО в Югославии (1999).

В ходе подготовки и проведения США и Великобританией военной операции против Ирака (2003г.) одну из ключевых ролей сыграло ее тщательное и заблаговременное информационно-психологическое обеспечение (ИПО).

Одной из первостепенных задач этой операции явились реализация положений концепции информационной войны и проведение психологических операций на стратегическом и оперативно-тактическом уровнях. В мероприятиях по ИПО агрессии против Ирака были комплексно задействованы официальные информационно-пропагандистские структуры и СМИ. Основными объектами информационно-психологического воздействия являлись мировое общественное мнение, собственное население, а также военно-политическое руководство, вооруженные силы и население Ирака.

Анализ мероприятий информационного обеспечения военной операции США и Великобритании против Ирака позволяет сделать вывод, что, несмотря на огромный потенциал и опыт ведения информационной войны, накопленный информационными структурами вооруженных сил США за последние несколько десятилетий, их эффективность оказалась значительно ниже той, которая была достигнута в 1991 г. в ходе операции "Буря в пустыне". Превосходства в медийно-информационной сфере американско-британским информационными структурами достичь не удалось. Наличие альтернативных и оппозиционных коалиционным информационным каналов (таких как "Euronews" в Европе и "Аль-Джазира" на Ближнем Востоке) во многом оказывало негативное и нейтрализующее воздействия на информационные усилия американско-британской коалиции.

Результаты социологического опроса, проведенного в 35 странах мира летом 2006 г., показали, что большинство опрошенных из 33 стран убеждены, что проводимая США война в Ираке привела к росту террористической угрозы.

В среднем 60% опрошенных в каждой из 33 стран согласны с тем, что оккупация Ирака в марте 2003 года увеличила вероятность террористических актов, в обратном уверены 12 %, сообщило Агентство Франс-пресс.

Информационная война на начальном этапе операции против Ирака была проиграна за счет того, что большинство мировых агентств и СМИ, исходя из позиций своих стран, фактически оказывали нейтрализующее воздействие на попытки информационного доминирования США и Великобритании в освещении боевых действий. США также оказались в информационной зависимости оправдывать цели войны после того, как по завершении операции ОМП в Ираке так и не было найдено.

Информационные структуры США оказались не готовы к высокому уровню информационного противодействия со стороны соответствующих структур Ирака. В частности, массированную кампанию по дезинформации

пришлось прекратить ввиду того, что большинство фактов быстро опровергалось, что негативно сказывалось на авторитете американских и британских информантств

В целом, можно выделить несколько этапов использования СМИ в очаговых вооруженных конфликтах

- Подготовительный,
- Основной,
- Заключительный

Новые тенденции в области средств и способов ведения войны, вызванные развитием информационных технологий, настолько фундаментальны и масштабны, что позволяют военным аналитикам говорить о новой революции в военном деле. Такая революция не сводится к количественному наращиванию технических характеристик вооружений и появлению новых технологических решений уже существующих задач в деле обеспечения национальной безопасности. Она предполагает также трансформацию способов и методов применения отдельных типов вооружений и их комбинаций, структуры и форм организации военного дела и, в конечном счете, новое концептуальное понимание целей и задач оборонной политики. Непрямыми, но политически крайне значимыми следствиями этой революции являются изменения в приоритетах бюджетных расходов на оборону и национальную безопасность, в формах и методах взаимодействия и координации в рамках “силового” блока государственных ведомств, в отношениях между военно-политическими институтами и обществом, а также в ряде других сфер.

В третьей главе – “Стратегическая информационная война” определяется сущность и структура стратегической информационной войны, рассматривается ее роль как явления современной политической действительности и значение в системе противоборства государств. Выявлены и описаны новые приоритеты в информационной безопасности США. Проанализированы современный опыт и тенденции развития информационно-психологического противоборства.

Понятие стратегической информационной войны (СИВ) включает в себя не столько использование информационных технологий для обеспечения традиционных военных действий, сколько асимметричное воздействие на те сегменты национальной информационной инфраструктуры противника, нарушение работоспособности которых может вызвать последствия, сопоставимые с результатами традиционных военных действий. Возможными последствиями СИВ могут явиться политический и экономический коллапс

страны, выход из строя объектов энергоснабжения, остановка транспорта и т.д.

К числу характерных признаков (критериев), позволяющих говорить о начале стратегической информационной войны, относятся

- наличие угрозы экономической безопасности государства,
- возникновение угрозы для проведения в жизнь национальной военной стратегии государства

В качестве основных средств ведения стратегической информационной войны могут выступать рассмотренные выше элементы информационных операций и террористических действий. При этом вновь возникает и упомянутая ранее проблема, связанная с тем, что ведение стратегической информационной войны, также как и борьба с терроризмом, подразумевает сложность выявления и идентификации противника, а в случае, если это будет сделано, то сложность выработки адекватных ответных мер.

Тем не менее, при успешной идентификации противника (государства-агрессора) появляется возможность сформулировать эффективную стратегию противодействия.

По мнению ряда экспертов, сдерживание может стать таким же действенным при ведении стратегической информационной войны, как и ядерное сдерживание времен «холодной войны». Поэтому, неудивительно, что стратегия сдерживания в информационном противоборстве во многих аспектах совпадает со стратегией ядерного сдерживания. Вместе с тем она подразумевает также целый ряд элементов, увязка которых с реалиями обеспечения информационной безопасности представляется затруднительной. Во-первых, должна существовать четко декларируемая политика, устанавливающая спектр ответных действий, которые могут быть применены к агрессору. Во-вторых, должна существовать возможность идентификации как источника информационной атаки, так и самого факта агрессии, сложность чего была показана выше. В-третьих, должна быть эксплицитно выражена готовность к ответным действиям, способным нанести неприемлемый ущерб агрессору. И, наконец, сдерживание должно восприниматься агрессором как вполне реальное и неизбежное.

Только в случае выполнения этих условий сдерживание может считаться эффективным. Однако при постоянном изменении спектра угроз в информационной сфере и, соответственно, при быстрой эволюции взглядов на защиту информационных инфраструктур осуществление стратегии сдерживания оказывается затруднительным. Вместе с тем западные эксперты считают, что несмотря на существующие ограничения, стратегия сдерживания может применяться уже в настоящее время на государственном уровне по отношению к основным международным конкурентам и соперникам в

информационной области, способным к ведению такого рода войны

Ниже рассматриваются основные принципы, которым должна соответствовать стратегия сдерживания в информационной сфере

- воля к ответным действиям,
- вероятность и уверенность,
- гарантированное взаимное уничтожение,
- недопущение СИВ,
- определение потенциального агрессора;
- система «раннего предупреждения» в информационном контексте,
- использование наступательных технологий

По мнению американских экспертов, сегодня необходима новая парадигма – «ноополитика» Это форма политического руководства, которая взаимодействует с ноосферой – самым широким информационным пространством сознания, в котором объединено киберпространство Ноополитика – это метод реализации внешней политики в информационную эпоху, подчеркивающий первенство идей, духовных ценностей, моральных норм, законов и этики, основанный на применении «мягкой», а не «грубой» силы Особо подчеркивается, что руководящим мотивом ноополитики не могут быть национальные интересы, определенные в терминах государственности Национальные интересы по-прежнему будут играть важную роль, но они должны быть определены больше в общечеловеческом, а не государственном масштабе и быть интегрированы с более широкими, даже глобальными, интересами в расширяющуюся транснациональную сетевую «структуру», в которую внедрены участники международных отношений

Таким образом, можно констатировать факт начала проведения изменений в области внешней и внутренней политики США в информационную эпоху Основной концепцией является информационная стратегия, а одним из ее компонентов будет Стратегическая информационная доктрина, как главный концептуальный документ реализации принципов информационного противоборства на поле боя в конфликтах новой эпохи

Заключение. Проведенное исследование позволило рассмотреть взгляды военно-политического руководства США на информационное противоборство и его ведение в рамках информационных операций вооруженных сил США Отражены различные этапы зарождения, становления и развития теории и практики информационной борьбы в масштабах всего государства и в рамках вооруженных сил США

В результате проведенного исследования диссертант пришел к следующим выводам

1 Современные идеи и материальные основы информационного противоборства формировались одновременно с развитием глобальной информационной среды, информационной сферы общества. Руководству США в середине 90-х годов стала очевидна необходимость разработки единой национальной информационной стратегии, которая получила воплощение в создании ряда структур, чья деятельность состояла в выработке предложений, позволяющих принимать контрмеры против угроз в быстро меняющейся информационной и технологической средах.

2 На межгосударственном уровне, США, имеющие богатый опыт и отработанную систему осуществления информационно-психологического воздействия (управления восприятием), проверенную в годы «холодной войны» и отработанную в ходе локальных войн и вооруженных конфликтов, стали адаптировать ее в новых международных условиях. Параллельно с этим реализовывались информационно-технические аспекты воздействия на информационные ресурсы и информационные системы, не позволяющие потенциальным противникам использовать технологические инновации в конкурентных целях.

3 Появление и динамичное развитие глобальных информационных сетей, основанных на передовых электронных технологиях, позволили США использовать их потенциал в решении различного рода государственных задач. Управляемое формирование глобального информационного пространства на основе новейших технологий в максимальной степени отвечало интересам США. Одновременно растущая зависимость США от информации и информационных систем и связанная с этим их уязвимость стали создавать широкий спектр угроз для национальной безопасности. С учетом этих угроз получили развитие оборонительные аспекты информационного противоборства.

Масштабное внедрение достижений информационных и телекоммуникационных технологий во все сферы жизнедеятельности государства и общества в США подтолкнуло к разработке государственных и военных программ по защите своих национальных интересов в информационной сфере. К началу XXI века в США насчитывалось более 40 специально созданных организаций, участвующих в информационном противоборстве.

4 Итоги военных действий в Персидском заливе в 90-х годах подтвердили важность формирования в интересах вооруженной борьбы необходимого информационного пространства. Главным уроком названных выше операций стало понимание, что информационное противоборство может и должно быть неотъемлемой составляющей эффективной государственной

политики Эта идея в политически корректных выражениях стала реализовываться на всех государственных уровнях США в 90-х годах XX века

5 Важный фактор, обеспечивающий превалирующее положение США в военной области, - это превосходство американских вооруженных сил над потенциальными противниками или союзниками на ключевых направлениях военно-технического прогресса Значительный прорыв науки в развитии новых перспективных технологий, а также успех промышленности в воплощении этих достижений уже сегодня ставят вооруженные силы США по их военно-техническому оснащению на уровень требований XXI Военно-политическое руководство, осознав значение потенциала новейших систем боевого управления, связи, компьютеров и разведки, сделало приоритетным достижение информационного превосходства над противниками в вооруженных конфликтах любой интенсивности и любого уровня Под информационным превосходством стали понимать способность к сбору, обработке и распространению непрерывного потока исчерпывающей и достоверной информации, одновременно затрудняя или воспрепятствуя аналогичные действия противника Для достижения информационного превосходства было сформулировано два условия во-первых, стремительно развивающиеся коммерческие технологии необходимо использовать и адаптировать их для нужд обороны быстрее, чем это делают военные конкуренты США, во-вторых, государству необходимо иметь эффективные наступательные и оборонительные информационные возможности, которые должны защищать информационные ресурсы и системы от нападения и обеспечивать соразмерные ответные действия

6 На рубеже XX и XXI веков информационное противоборство в сфере обеспечения национальной безопасности Соединенных Штатов Америки, особенно в вооруженных силах, выходит на первый план в общей системе различных видов борьбы, в том числе вооруженной Используя весь предшествующий опыт подготовки и ведения локальных войн и вооруженных конфликтов, США в 90-е годы осуществили прорыв в теории и практике комплексного применения сил и средств психологических операций, радиоэлектронной борьбы, введения противника в заблуждение, противодействия разведке противника, специальных операций нападения на компьютерные сети, а также в разработке способов эффективного применения службы по связям с общественностью и службы по работе с гражданской администрацией, объединив их усилия для практической реализации современной концепции информационного противоборства – концепции информационных операций (документы КНШ МО США "Единые перспективы 2010" и "Единые перспективы 2020" , а также документы МО США

"Четырехлетний обзор состояния вооруженных сил" от 2001 и 2006 годов) Участие вооруженных сил США в локальных войнах и вооруженных конфликтах в конце XX века позволило им накопить опыт использования современных технологий информационного противоборства

7 Как показало исследование, современный потенциал системы информационного противоборства американских вооруженных сил является воплощением развития теоретических взглядов, всего исторического опыта совершенствования ее информационно-психологических и информационно-технических компонентов, применения самых разнообразных форм и способов воздействия на важнейшие информационные ресурсы и системы вооруженных сил и государств потенциального противника Анализ зарождения и развития концепции информационных операций американских войск на протяжении более чем пятидесяти лет позволил диссертанту проследить совершенствование теории и практики указанных компонентов, дать объяснение существующей ныне структуры аппарата, механизма и специфики системы проведения информационных операций вооруженных сил США, тенденции их дальнейшего развития Уже в начале 90-х годов на примере опыта войны в Персидском заливе стало очевидно, что произошло слияние информационно-психологической и информационно-технической составляющих информационного противоборства Достижение информационного превосходства потребовало особых инструментов, позволяющих воздействовать на всю информационную сферу противника В свою очередь они получили развитие в рамках концепции информационных операций, основанной на полученном опыте информационного противоборства при проведении военных действий вооруженными силами США в конце XX века

В результате исследования автор пришел к заключению, что структура и механизм проведения информационных операций окончательно сформировались в вооруженных силах США только во второй половине 90-х годов Детальное изучение особенностей информационного противоборства, его содержания, форм и методов, доктринальных разработок, способов их практической реализации позволяет диссертанту утверждать, что информационные операции стали неотъемлемой частью деятельности вооруженных сил США как в мирное время, так и при проведении военных действий

8 В настоящее время США по сравнению с другими странами обладают значительным преимуществом в области разработки и использования информационных, телекоммуникационных технологий, а также различного рода радиоэлектронных систем Основываясь на концепции информационных

операций, военно-политическое руководство США стремится всячески закрепить за собой доминирующую роль не только в политической, экономической и военной сферах, но и в мировой информационной инфраструктуре. Об этом свидетельствует характер и специфика ведения информационного противоборства в деятельности американских войск последнего десятилетия XX века.

9 Изучение опыта информационного противоборства американских вооруженных сил в конце XX века, а также руководящих документов военно-политического руководства США позволяет утверждать, что достижение информационного превосходства – это главный ориентир на перспективу до 2020 г. Сегодня военно-политическое руководство США делает ставку не столько на современные системы огневого поражения и высокоточное оружие, сколько на сохранение и использование в полном объеме своего информационного превосходства.

10 Анализ содержания, форм и методов информационно-психологического и информационно-технического воздействия на войска и население противника, мировую общественность и население своей страны, а также обобщение теоретического и практического опыта информационных операций американской армии в конце XX века имеют важное значение и для творческого осмысления этих проблем в Российской Федерации.

11 Как выяснилось в процессе исследования, концепция информационного противоборства в том виде, в каком она реализуется в вооруженных силах США, для российского военного искусства не является чем-то новым. Теоретические основы информационно-психологического и информационно-технического противоборства довольно полно разработаны в отечественной военной науке. Они раскрываются через такие понятия, как «борьба с системами управления противника», «радиоэлектронная борьба», «завоевание господства в эфире», «психологическая борьба», «оперативная и стратегическая маскировка войск», «дезинформация» и другие.

Новизна американского подхода к теории и практике информационного противоборства состоит в комплексном использовании прежних, в том числе и российских, военно-теоретических разработок по данной проблематике и новейших достижений в области информационных технологий, психологии, социологии, этнологии и других наук, возможностях их применения на всех уровнях государственного и военного управления.

Теоретические обобщения и выводы, сделанные в работе, изложены в следующих публикациях автора

1 "Сетевая война" – новый вид противоборства//Обозреватель-Observer – Москва – 2007 - №10 – 0,5 п л – **Издание из перечня ВАК.**

2 Экономическая информационная война //Внешнеэкономические связи – Москва – 2007 - №2 – 0,5 п л