

На правах рукописи



005005265

Соловьева Елена Александровна

**ИНФОРМАЦИОННОЕ ПРОТИБОБОРСТВО В СЕТИ
ИНТЕРНЕТ: ПОЛИТОЛОГИЧЕСКИЙ АНАЛИЗ**

Специальность 23.00.02 –
Политические институты, процессы и технологии
(политические науки)

Автореферат
диссертации на соискание ученой степени
кандидата политических наук

- 8 ДЕК 2011

Пятигорск - 2011

Диссертация выполнена на кафедре международных отношений, мировой экономики и международного права ФГБОУ ВПО «Пятигорский государственный лингвистический университет»

Научный руководитель: доктор политических наук, профессор
Панин Виктор Николаевич

Официальные оппоненты: доктор политических наук, профессор
Чагилов Валерий Расулович

кандидат социологических наук,
доцент **Гапич Александр Эрикович**

Ведущая организация: **ФГБОУ ВПО «Ставропольский государственный университет»**

Защита состоится 23 декабря 2011 года в 17-30 на заседании диссертационного совета Д 212.193.03 при ФГБОУ ВПО «Пятигорский государственный лингвистический университет» по адресу: 357532, г. Пятигорск, пр. Калинина, 9, конференц-зал № 1

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВПО «Пятигорский государственный лингвистический университет».

Автореферат разослан «22» ноября 2011 г.

Ученый секретарь
диссертационного совета



Г.В. Косов

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования определяется тем, что в настоящее время электронное пространство в большинстве случаев повторяет реальную сферу политики, знаменуя собой глубокую степень проникновения Интернет-технологий в политическую жизнь общества.

Влияние виртуального пространства на международный, национальный, региональный политический процесс обуславливают стремление современных государств к освоению и использованию новых ресурсов.

В современных военно-политических конфликтах ведущие мировые державы активно используют Интернет, трансформируя и модифицируя с его помощью функциональные возможности органов военного управления, делая их более гибкими. Однако угрозы и масштабы последствий, которые влечет за собой эта трансформация, и усиление государственной сетевой борьбы остаются малоизученными, что актуализирует тему данного исследования.

Такие особенности виртуального пространства, как децентрализованная система, отсутствие правового поля регулирования сети, детерминируют процесс манипулирования общественным мнением, электоральными волеизъявлениями россиян, что является угрозой личной и общественной безопасности. Минувя традиционные политические институты государства, воздействуя напрямую на гражданина - пользователя сети - посредством форумов, блогов и социальных сетей, Интернет становится эффективным механизмом влияния и манипулирования. Выработка методов и механизмов противодействия этим процессам придает теме данной диссертационной работе дополнительную актуальность.

Выявление потенциальных угроз виртуального пространства, а также анализ возможностей применения ресурсов сети в процессе ведения информационного противоборства имеют большое значение для Российской Федерации с точки зрения выработки адекватных мер противодействия негативному информационному влиянию в Интернете в целях обеспечения национально-государственной, общественной и личной безопасности, что делает тему диссертационного исследования актуальной.

Таким образом, приведенная аргументация и заявленная проблема имеет как научно-теоретическое, так и практическое значение, что и обусловило выбор темы.

Степень научной разработанности проблемы. Общим вопросам теории безопасности и национальной безопасности в частности

посвящены труды современных зарубежных исследователей Д. Бейтса, С. Джоунса, Л. Зеднер, Д. Кеннеди, К. Кэмпбелла, Р. Ли, М. О'Хэнлона.

Национальная безопасность Российской Федерации исследовалась такими отечественными учеными, как П.В. Акинин, М.А. Аствацатурова, А.А. Башкунов, В.С. Белозеров, А.А. Вартумян, А.В. Возжеников, М.И. Дзалиев, З.А. Жаде, Н.П. Медведев, Л.А. Михайлов, Г.В. Косов, В.Н. Панин, С.В. Передерий, С.И. Петров, А.А. Прохожев, А.Д. Урсул, С.А. Фомин, И.В. Юрченко и др.

Информация как философский феномен, информация в структуре политической коммуникации рассматривалась зарубежными (Н. Винер, П. Лазарсфельд, Н. Луман, М. Маклюэна, М. Маккомбс, Р. Мертон, Ю. Хабермас, Д. Шоу) и отечественными (М.А. Василик, М.С. Вершинин, Л.А. Волова, О.Л. Гнатюк, М.Н. Грачев, Л.М. Землянова, В.И. Каширин, А.И. Соловьев, Л.Н. Федотова, М.М. Шульга) исследователями.

Осмыслению феномена информатизации современного общества и изучению содержания процесса формирования информационного общества посвящены работы зарубежных теоретиков Д. Белла, Ф. Вебстера, М. Кастельса, Е. Масуда, К. Мзя, Э. Тоффлера, А. Турена, Ф. Уэбстера, Р. Хассана, А. Этциони и др.

Особое место занимают исследования, в которых теоретико-методологические обобщения конкретизированы относительно проблем информационной безопасности. К ним, в первую очередь, необходимо отнести труды Н.А. Брусницына, В.Б. Вербенко, Е.А. Ерофеева, Д.П. Кафтанчикова, С.А. Клейменова, Б.Г. Койбаева, А.В. Крутских, Ю.В. Лучинского, В.П. Мельникова, И.Л. Морозова, А.М. Петракова, Ю.С. Уфимцева, А.Н. Федорова, Д.Ю. Швец, В.И. Ярочкина и др., в которых представлены основные положения информационной безопасности деятельности государства и его политической системы.

Следующую группу представляют работы отечественных (О.А. Алимуратов, О.В. Иванников, И.Э. Калоева, Е.В. Кипрская, А.В. Манойло, Д.П. Прудников, С.В. Сидорова, Л.Я. Сухотерин, И.В. Юдинцев, С.В. Хребина, В.Р. Чагилов, А.А. Чертополох) и зарубежных (Б. Волтер, А. Гор, М. Дейви, М.Кахлер, Дж. Клэппер, В. Майер-Шенбергер, Д. Миршаймер, С. Мюрден, Е. Персе, Д. Хёрли) ученых, в которых анализируются состояние и перспективы использования информации, информационных средств и технологий для достижения политических и военно-стратегических целей государства, раскрывающие сущность информационного противоборства.

Технологии, средства и методы информационного противоборства обстоятельно исследованы в научных трудах российских (С.Н. Бухарин, В.Б. Вепринцев, Н.Л. Волковский, Л.В. Воронцова, А.Г. Караяни, В.А. Лисичкин, А.В. Манойло, И.Н. Панарин, Л.Г. Панарина, А.И. Петренко, Г.Г. Почепцов, С.П. Расторгуев, С.С. Сулакшин, В.В. Цыганов, Л.А. Шелепин) и зарубежных (П. Лайнбарджер, Г. Ласвель, Д. Конерри, Д. Най, К. Стюарт, О. Тоффлер, Р. Шафрански, В. Швартау, Т. Томас, У. Тоши) исследователей. Данные работы включают анализ широкого спектра вопросов информационного противоборства в политике современных государств, в том числе и некоторые аспекты основ ведения информационной борьбы с использованием ресурсов Интернета.

Анализом политической составляющей глобальной сети Интернет занимались Д.С. Барина, Д.В. Войнов, А.А. Киселев, Н.В. Кондрашиной, О.И. Лосенкова, О.Д. Натсак, Д.Н. Песков, А.В. Роменков, Н.В. Соленикова.

Д.В. Акаев, И.В. Андреев, И.В. Василенко, А.Е. Войкунский, Г.В. Грачев, С.Г. Кара-Мурза, Ю.М. Кузнецова, И.К. Мельник, Е.А. Путилова, М.В. Реуцкий, О.Г. Филатова, Т.В. Филиппова, Н.В. Чудова, В.Ю. Шалак, А. Н. Шерemet рассматривали манипулятивные и политтехнологические возможности глобальной сети.

Политико-правовой аспект регулирования Интернет-пространства исследован в трудах Т.А. Биячueva, Я.Н. Засурского, Е.С. Зиновьевой, М.А. Зубовой, Н.В. Исаков, В.А. Копылова, Е.В. Михайленко, О.В. Мозолина, С.В. Молчанова, В.Б. Наумова, И.М. Рассолова, А.И. Савельева и др.

Технологиям применения политическими акторами сети Интернет в информационном противоборстве посвящены научные изыскания В.Р. Ахмадуллина, А.Э. Гапича, О.Н. Забузова, С.С. Игнатовой, Д.А. Лушников, И.А. Пенькова, А.В. Чугунова. К наиболее значимым зарубежным исследованиям по данной тематике можно отнести труды М. Либики, М. Камата, Д. Мэтиасона, Дж. Рэтрeя, Р. Хейни.

Исследуемая проблема освещается в ряде диссертационных работ таких авторов, как А.В. Атанесян, К.Ю. Будылин, А.Л. Бутенко, И.А. Быков, Б.В. Вербенко, А.Н. Горбенко, А.Л. Деньщиков, О.Н. Пирущий, А.Н. Резник и др.

В целом, отдавая должное теоретической глубине, обстоятельности, разносторонности научных исследований и признавая вклад всех вышеуказанных, а также других авторов в развитие теоретико-методологических основ политической теории информационного противоборства, следует отметить, что особенности и технологии полити-

ческой составляющей информационного противоборства современных акторов в сети Интернет в отечественной науке не получили достаточного научного осмысления, что и обусловило выбор данной проблематики в качестве темы данного исследования.

Объектом исследования являются политические аспекты информационного противоборства в сети Интернет.

Предмет исследования – информационное противоборство в сети Интернет как угроза/условие обеспечения информационной безопасности РФ.

Целью работы является выявление сущности современного информационного противоборства, особенностей его ведения в виртуальном пространстве и разработка механизмов обеспечения информационной безопасности РФ в сети Интернет.

Достижение поставленной цели предполагает постановку и решение следующих задач:

- уточнить сущность информационного противоборства как категории политической науки;
- доказать, что в ситуации глобализирующегося мира глобальная сеть Интернет становится инструментом политического манипулирования;
- охарактеризовать и систематизировать основные политические Интернет-технологии информационного противоборства;
- выявить базовые элементы российской государственной системы информационного противоборства в сети Интернет;
- определить современные Интернет-стратегии и технологии информационного противоборства России;
- предложить способы и технологии повышения эффективности ведения информационного противоборства в сети Интернет России.

Теоретико-методологической основой исследования послужили структурный, системный, сравнительный, прогностический и конфликтологический подходы, которые сделали возможным изучение объекта и предмета исследования в комплексе, выявление их наиболее существенных элементов, а также взаимозависимости и взаимообусловленности между ними.

Методологические основания исследования включают в себя методологические принципы политической коммуникативистики (А.И. Соловьев, М.А. Василик, М.С. Вершинин, Н. Винер, К. Шеннон, Г. Маклюен), теорию коммуникативного действия Ю. Хабермаса, теорию «постановки повестки дня» М. Маккомбса и Д. Шоу, критическую теорию массовых коммуникаций «спираль молчания» Э. Ноэль-Нойманн, концепцию обоснования как коммуникативного механизма легитимации власти и

принимаемых политических решений (А.В. Атанесяна). Использование данных теорий в диссертационном исследовании способствовало выявлению механизмов управления массовым сознанием, стратегий воздействия на общественное мнение в процессе информационного противоборства и оценки их эффективности.

Методы исследования. Достижению цели исследования и успешному разрешению поставленных задач способствовал ситуационный анализ практического опыта применения Интернет-технологий информационно-психологического и информационно-технического противоборства в рамках проблемного и диагностического полей, методы индуктивного обобщения, компаративного, факторного и геополитического анализа.

Применялись контент-анализ и компаративный анализ публикаций разных видов онлайн-СМИ, на материалах которых исследовались современные технологии информационного противоборства. Посредством семантико-лексической экспертизы политических текстов, способствовавшей выявлению механизмов формирования образа объекта через подбор фактов, негативных коннотаций и оценочных суждений, транслирующихся через семантико-лексические единицы, поддающиеся точному подсчету, был проведен анализ сетевых манипулятивных и пропагандистских технологий семантического манипулирования как инструмента воздействия на общественное сознание.

Эмпирическая основа исследования может быть сгруппирована следующим образом. Первая группа источников состоит из доктринальных документов в сфере информационного противоборства и безопасности Российской Федерации, а также основных законодательных актов, регулирующих применение Интернета в России.

Вторую группу источников составили международные документы, регламентирующие развитие Интернет-технологий. К ним, прежде всего, относятся конвенции и декларации таких межправительственных организаций и структур, как ООН, «Группа восьми», Европейского Союза, ШОС и ряда других.

В третью группу включены ресурсы сети Интернет: материалы анкетных опросов и результаты социологических и политологических исследований, проведенных профессиональными социологическими центрами (ВЦИОМ, ФОМ, TNS); мониторинги и аналитические разработки научно-исследовательских институтов и организаций, специализирующихся на вопросах управления Интернетом; материалы отечественных и зарубежных информационных агентств, информационно-аналитических Интернет-порталов; блогов, официальных сайтов органов государственной власти Российской Федерации.

Научная новизна диссертационного исследования состоит в следующем:

- дано авторское определение информационного противоборства как многоуровневой государственной системы информационного воздействия с целью обеспечения информационной безопасности, сформулированы основные закономерности информационной составляющей современных политических коммуникаций и доказано, что стратегии информационного противоборства могут быть применены на любом уровне организации политической власти;

- доказано, что в ситуации глобализирующегося мира Интернет становится эффективным средством информационно-психологического воздействия и политического манипулирования и что глобальная сеть выступает одним из инструментов современной политической борьбы между различными субъектами политики;

- определены сущность и специфика информационного противоборства в сети Интернет, выявлены объекты информационной борьбы, посредством систематизации которых проведена классификация основных политических технологий информационного противоборства в сети Интернет;

- дана характеристика современной российской системе информационного противоборства в сети Интернет, определены механизмы ее функционирования и обосновано влияние государственно-правовых механизмов управления Интернет-пространством на состояние информационной безопасности РФ;

- выявлены стратегии информационного противоборства и рассмотрен практический опыт применения современных политических Интернет-технологий информационного противоборства России;

- сформулирована и обоснована авторская концепция кибербезопасности и предложен комплекс мер по ее обеспечению.

Положения, выносимые на защиту:

1. Информационное противоборство представляет собой совокупность взаимоотношений акторов политической системы общества, в рамках которой путем активного воздействия на информационную сферу друг друга субъекты информационной борьбы стремятся получить превосходство над противоборствующей стороной в политической, экономической, военной и других областях. В современных условиях эффективное использование стратегий информационного противоборства дает возможность субъектам политики решать свои политические задачи в системе информационного пространства на всех уровнях организации власти как в горизонтальной (региональный, национальный, глобальный уровни), так и в вертикальной (личный, общественный, государственный) плоскостях.

2. Основными особенностями глобальной сети, формирующими пространство для политического манипулирования и позволяющими рассматривать Интернет в качестве самостоятельного инструмента современной политической борьбы различных субъектов политики, являются децентрализованная структура; отсутствие официальной цензуры, свобода распространения и получения информации; высокая скорость передачи данных; возможность воздействия на конкретную узкопрофильную аудиторию; отсутствие территориальных и временных ограничений; невысокая стоимость коммуникации. Выявленные преимущества виртуального пространства обуславливают активное использование политическими акторами глобальной сети для решения своих задач посредством политического манипулирования, пропаганды, контрпропаганды, дезинформации, через воздействие на общественное сознание актора-оппонента с целью навязывания определенных идей, ценностей, форм поведения и т.д.

3. Под «информационным противоборством в сети Интернет» понимается соперничество политических акторов посредством использования специальных информационно-технических ресурсов Интернета для воздействия на информационную среду противостоящей стороны, влияния на ее аудиторию и различные сферы политико-властных отношений с целью установления контроля над источниками виртуальных и электронных стратегических ресурсов противника и достижения информационного превосходства. В процессе информационной борьбы в виртуальном пространстве глобальной сети противоборствующие субъекты политики оперируют технологиями воздействия на социально-психологические и технические ресурсы друг друга, используя в первом случае информационно-психологическое, пропагандистское влияние и манипулирование общественным сознанием, а во втором – специфические атакующие технологии.

4. Российская государственная система информационного противоборства представляет собой централизованный, согласованный и целенаправленный комплекс мероприятий и механизмов органов власти РФ, направленный на защиту государственных интересов и обеспечение личной, общественной и национальной безопасности России в сети Интернет. Механизмы информационного противоборства современной России в сети Интернет связаны с противодействием информационной агрессии на ранних стадиях информационной конфронтации; реакцией на внезапные мероприятия информационно-психологической агрессии; профилактикой и прогнозированием; системой сил и средств информационного воздействия и противодействия; правовым обеспечением сферы управления Интернет-пространством.

5. Современные стратегии информационного противоборства России в сети Интернет представляют собой комплекс мероприятий, реализуемый по трем основным направлениям деятельности: информационное воздействие на массовое сознание, целью которого является изменение поведения людей и навязывание им целей, не входящих в число их интересов; информационное противодействие негативному информационному влиянию в сети Интернет в целях обеспечения психологической защиты населения страны и обеспечения информационной безопасности и стратегический политический анализ, включающий реализацию диагностической, аналитической, прогностической, управленческой, профилактической и коррекционной функций. Существующие на данный момент стратегии информационного противоборства России на практике оказываются малоэффективными в виртуальном пространстве сети Интернет.

6. Современные угрозы личной, общественной, национальной безопасности, генерируемые несистемными акторами политического процесса, детерминируют разработку концепции кибербезопасности, суть которой заключается в минимизации рисков политической и социальной стабильности, исходящих из Интернет - пространства. Основными механизмами реализации данного вида безопасности являются формирование скоординированной информационной политики органов государственной власти по отношению к виртуальному пространству и противодействию негативному информационному влиянию в сети; развитие российского сегмента Интернет; создание общественного Центра обработки данных об угрозах в Интернете и т.д.

Теоретическая значимость работы заключается в том, что определенные результаты исследования способствуют расширению категориального аппарата политической науки: в работе уточнено содержание таких теоретических понятий, как информационное противоборство, политические Интернет-технологии, политическое манипулирование, кибербезопасность и др. Выводы, полученные в ходе исследования, создают теоретическую базу для дальнейшего изучения вопросов реализации национальных интересов Российской Федерации в сети Интернет как элемента обеспечения национальной безопасности России и основ ведения информационного противоборства в виртуальном пространстве глобальной сети на всех уровнях организации государственной власти.

Практическая значимость исследования состоит в том, что представленные материалы и результаты анализа сущности и технологий информационного противоборства могут быть применены в практической деятельности государственных политических структур, аналитических центров Российской Федерации, общественно-политических объединений при разработке различных концепций ведения информационного

противоборства, мероприятий противодействия негативному информационному влиянию в сети Интернет, выработки совместных механизмов информационной защиты от угроз виртуальной среды посредством организации эффективного информационного взаимодействия органов власти с населением и бизнес-структурами.

Материалы и выводы работы также могут быть использованы в учебном процессе в вузах при подготовке и чтении таких дисциплин, как «Информационная безопасность России», «Информационное обеспечение внешней политики РФ», «Мировые информационные ресурсы», «Информационные технологии в прогнозно-аналитической деятельности» и др.

Апробация работы. Основные положения работы излагались в докладах и сообщениях в Летней школе международных отношений «Вызовы и угрозы безопасности: региональный и международный аспекты» (г. Волгоград, 2006); на XX сессии Летнего методологического института международных отношений «Ресурс сопредельных пространств в мировой политике» (г. Смоленск, 2007 г.); V Международном конгрессе «Мир на Северном Кавказе через языки, образование, культуру» (г. Пятигорск, 2007); в Летней международной школе – 2008 «Балтийско-черноморский регион: перспективы региональной безопасности после саммита НАТО в Бухаресте» (п. Лосево, Ленинградская область, 2008 г.); на Международных молодежных конференциях Ассоциации Евроатлантического сотрудничества «Евроатлантическая безопасность: провал или реформы» (г. Москва, 2008 г.); «Евроатлантическая безопасность перед лицом новых вызовов и угроз» (г. Москва, 2009 г.); Международном молодежном форуме «Новые правила: стратегия мировых взаимоотношений» (п. Дагомыс, Краснодарский край, 2009 г.); в Международной летней школе молодых исследователей «Политические и социальные процессы в евразийском пространстве: в ожидании новых парадигм» (Республика Армения, г. Цахкадзор, 2009 г.); на VI Международном конгрессе «Мир через языки, образование, культуру: Россия – Кавказ - мировое сообщество» (г. Пятигорск, 2010 г.); Международном Российско-Балтийский форуме молодых лидеров - 2011 «Принятие дальнейших шагов в обеспечении европейской и региональной безопасности» (Эстонская Республика, г. Таллинн, 2011 г.); во Всероссийской научно-практической конференции: «Образ кавказца в центральной прессе: проблемы и решения» (г. Махачкала, 2008 г.); Региональной конференции Кавказской сети Глобального партнерства по предотвращению вооруженных конфликтов (г. Пятигорск, 2011 г.), а также в рамках 10 межрегиональных научно-практических конференций, проводи-

мых в Пятигорском государственном лингвистическом университете (г. Пятигорск, 2006-2011 гг.).

Основные результаты исследования получили свое отражение в 10 научных публикациях общим объемом 3,7 п.л., в том числе 2 из них были опубликованы в ведущих научных журналах, рекомендованном ВАК РФ для апробации итогов диссертаций.

Диссертация обсуждена на заседании кафедры международных отношений, мировой экономики и международного права ФГБОУ ВПО «Пятигорский государственный лингвистический университет» и рекомендована к защите по специальности 23.00.02 – Политические институты, процессы и технологии (политические науки).

Структура работы обусловлена целью, задачами и внутренней логикой исследуемой проблемы и состоит из введения, двух глав, включающих в себя 6 параграфов, заключения, библиографического списка использованной литературы, состоящего из 348 источников, в том числе 109 на иностранных языках, и 7 приложений. Общий объем работы составляет 167 страниц машинописного текста.

II. ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность исследуемой темы, оценивается степень её научной разработанности, определяются объект и предмет исследования, излагаются его цель и задачи, характеризуются теоретико-методологическая и эмпирическая основы диссертации, раскрывается её научная новизна, формулируются основные положения, выносимые на защиту, выявляется теоретическая и практическая значимость работы, приводится её апробация и дается характеристика структуры исследования.

В первой главе **«Теоретико-методологические основы исследования политической составляющей информационного противоборства в сети Интернет»** анализируются концептуальные подходы к исследованию феномена информационного противоборства (ИП) как категории политической науки, выявляются специфика и технологии его ведения в виртуальном пространстве сети Интернет.

В рамках первого параграфа первой главы **«Информационное противоборство» как категория современной политической науки»** на основе анализа исторических аспектов зарождения и развития информационного противоборства исследуется процесс становления информационно-психологических и дезинформационных средств и методов как самостоятельного инструмента решения политических задач государства, способствующих формированию современного системного видения терминологиче-

ской базы информационного противостояния и выявлению основных закономерностей информационной составляющей политической борьбы.

На основе исследования эволюции практического опыта (К. Стюарт, Г. Ласвель, П. Лайнбарджер) и теоретического содержания информационного противоборства (Л.В. Воронцова, А.В. Манойло, Д.Б. Фролов) делается вывод о том, что в процессе исторического развития информационно-психологическая деятельность государственных органов власти претерпела существенные изменения и в настоящее время превратилась в постоянно действующий фактор политики-информационное противоборство.

В современных условиях информационное пространство продолжает оставаться сферой постоянного противоборства различных субъектов политики на всех уровнях организации власти. Данный факт обуславливается тем обстоятельством, что информационные потоки, свободно пересекающие государственные границы, создают принципиально иную ситуацию в контексте функционирования государственной власти и ее институтов, а интеграция инфраструктур государства на основе информационных систем делает их потенциальными объектами информационной борьбы. В перспективе такая тенденция, ведущая к «информатизации» вооруженных сил и «интеллектуализация» традиционных вооружений (А.В. Крутских), будет способствовать расширению власти не за счет традиционной вооруженной борьбы, а в ходе борьбы за контроль над информацией и завоевание информационного господства.

Критическое осмысление категориального аппарата политической науки, семантически относящегося к категории «информационное противоборство» – «информационная борьба» (И.Н. Панарин), «информационное противостояние» (А.Г. Караяни), «информационная война» (Г.Г. Почепцов, С.С. Сулакшин), «психологическая война» (С.П. Расторгуев), «информационно-психологическая война» (А.В. Манойло), «война информационной эры» (В. Швартау) и др. – детерминирует вывод о том, что в отечественной и зарубежной науке не существует четкой дифференциации ряда понятий, относящихся к категории информационного противоборства, и зачастую многие из них используются как синонимы. Формулируется авторское понимание информационного противоборства, под которым понимается совокупность таких взаимоотношений субъектов политической системы общества, в рамках которых путем активного воздействия на информационную сферу друг друга акторы информационной борьбы стремятся получить превосходство над противостоящей стороной в экономической, политической, военной и других областях.

Во втором параграфе первой главы «Глобальная сеть как инструмент политического манипулирования» характеризуются манипулятивные возможности Интернета как средства информационно-психологического воздействия на общественное сознание, а также особенности самой глобальной сети, позволяющие рассматривать ее в качестве самостоятельного инструмента современной политической борьбы различных субъектов политики.

Современная система Интернет-пространства включает в себя технические, социальные и политические характеристики (Д.Н. Песков). В этой связи предлагается авторское определение политической составляющей глобальной сети: Интернет - это целостный социотехнический феномен, представляющий собой глобальную социально-коммуникационную сеть политической направленности, предназначенную для удовлетворения информационно-коммуникационных потребностей государства и иных политических акторов посредством использования сетевых коммуникационных технологий для реализации своих задач и интересов в сфере политико-властных отношений.

На основе исследования научной базы определения социально-политической роли (Е.А. Путилова, Т.В. Филиппова) и функций сети Интернет (С.А. Клейменов, В.П. Мельников, А.Н. Шеремет) в сфере политико-властных отношений, делается вывод о том, что характерные особенности сети Интернет (децентрализованная структура; отсутствие цензуры, свобода распространения и получения информации; интерактивность, оперативность и экономичность; возможность воздействия на конкретную узкопрофильную аудиторию; отсутствие территориальных и временных ограничений) позволяют использовать ее в качестве средства политического манипулирования, представляющего собой систему способов психологического воздействия на массы, которые политические власти используют с целью политического обмана, внедрения в сознание народа иллюзорных представлений о политической жизни.

Для реализации своих политических интересов при помощи Интернета манипуляторы могут использовать новые формы опосредованного социального контроля, основанные на замаскированном манипулировании сознанием, мягком подавлении психики. С практической точки зрения технологии виртуальной реальности позволяют сделать информационно-психологическое воздействие индивидуальным, ориентированным на манипуляцию сознанием конкретной личности.

Сила информационно-психологического воздействия в Интернете умножается многократно благодаря новым технологиям мультимедиа и виртуальной реальности, которые могут использоваться в

процессе политического манипулирования для воспроизводства модели реальной ситуации, имитации действительности, сочетая элементы реального видеозображения и элементы, созданные компьютерной графикой. Сама по себе имитация действительности также представляет собой своеобразный политический инструмент информационного воздействия на сознание и подсознание человека, способный спровоцировать у пользователей появление так называемой Интернет-аддикции, а людей, зависимых от виртуальной среды, - сделать наиболее уязвимыми объектами политического манипулирования.

В третьем параграфе первой главы **«Политические технологии информационного противоборства в сети Интернет»** дается авторское определение понятия «информационное противоборство в сети Интернет», исследуется его природа и механизмы включения в него современных политических акторов, содержание и характер их политики в данной области. Особое внимание уделяется исследованию политических информационно - манипулятивных и информационно-технических Интернет-технологий, составляющих сущность информационного противоборства в виртуальном пространстве Сети.

Под информационным противоборством в сети Интернет понимается соперничество политических акторов посредством использования специальных информационно-технических ресурсов Интернета для воздействия на информационную среду противостоящей стороны, влияние на ее аудиторию и различные сферы политико-властных отношений с целью установления контроля над источниками виртуальных и электронных стратегических ресурсов противника и достижения информационного превосходства.

Опираясь на положение о том, что Интернет представляет собой комплексное социотехническое явление, определяется, что объектами информационного противоборства в сети Интернет являются как социальные, так и технические ресурсы государства. В соответствии с этим выделяются два основных направления сетевого информационного противоборства – информационно-техническое (ИТП) и информационно-психологическое (ИПП), каждому из которых соответствует определенный набор Интернет-технологий (атакующих и манипулятивных).

Объектами ИТП являются информационно-технические системы управления (электронные и компьютерные связи и коммуникации), информационно-аналитические системы и собственно виртуальные информационные ресурсы. Выявляются основные политические технологии информационно-технического воздействия, применение которых способствует нарушению эффективности функционирования работы сети Интернет: 1) «бомбардировка» сети электронными письма-

ми; 2) DOS-атаки; 3) компьютерные вирусы; 4) «логические бомбы», «программы-оборотни», «программы-убийцы информации»; 5) компьютерные агенты - сети с элементами искусственного интеллекта (компьютерные боты (роботы); 6) средства внедрения вирусов (вирусные пушки и др.); 7) хакерство и другие нелегальные приемы воздействия.

Объектами информационно-психологического противоборства являются психика отдельной личности (организационные структуры формирования общественного сознания); психологические явления и процессы в социально-политических общностях различного масштаба, что и обуславливает выбор соответствующих технологий сетевого ИПП.

Рассматриваются основные политические Интернет-технологии ведения информационно-психологического противоборства, такие, как распространение пропагандистских информационных материалов с помощью различных технологий привлечения внимания, организации виртуальных групп по интересам, сбор адресов электронной почты для организации массовых рассылок, размещения баннеров на часто посещаемых сайтах; организации новостных групп; виртуальных групп по интересам; создания сайтов для обмена мнениями; размещение информации на отдельных страницах онлайн-изданий, регистрация в поисковых системах сайтов противоположного содержания по одинаковым ключевым словам, перенаправление (подмену) ссылок на другой адрес; семантические атаки; специальный вид хакерства (хакеры - «вербовщики») и т.д.

Наличие большого арсенала как атакующих, так и манипулятивных политехнологий, используемых различными субъектами политики в целях реализации своих политических задач, свидетельствует о том, что удельный вес виртуальной информационной составляющей в политике сегодня имеет устойчивую тенденцию к возрастанию и позволяет говорить о медиатизации политики и виртуализации политического пространства.

Во второй главе **«Информационное противоборство современной России в условиях информационно-коммуникативного пространства сети Интернет»** характеризуется современная российская модель информационного противоборства в сети Интернет, стратегии и технологии его ведения.

В первом параграфе второй главы **«Государственная система информационного противоборства в сети Интернет: опыт современной России»** определяются основные элементы и механизмы функционирования современной российской системы информационного противоборства в сети Интернет, исследуется нормативно – пра-

вовая база национального законодательства РФ в сфере управления Интернет-пространством как основа обеспечения информационной безопасности современной России.

Основные угрозы национальной безопасности РФ, связанные с глобальной сетью Интернет, заключаются в возможности применения интерактивных информационно-коммуникационных технологий в политических, военных целях, в террористической деятельности.

Основами функционирования российской системы информационного противоборства в сети Интернет являются механизмы противодействия информационно-психологической агрессии на ранних стадиях информационного противоборства; механизмы быстрого реагирования на внезапные мероприятия информационно-психологической агрессии; механизмы профилактики и прогнозирования; системы сил и средств информационного воздействия, а также правовые механизмы (правовая база национального законодательства РФ в сфере управления Интернет-пространством), формирующие основу государственной информационной политики России в условиях ИП в сети Интернет.

В настоящее время Российская Федерация не относится к категории стран, использующих передовые технические веб-фильтрации Интернет-контента. Тем не менее, уже сегодня в России существуют механизмы формирования онлайн-пространства в желательном для государства направлении при помощи платных блоггеров, влияния на основных Интернет-провайдеров и Интернет-компании, и правовой основы, которая позволяет РФ участвовать в надзоре за Интернетом, особенно в периоды повышенной политической напряженности.

В современных условиях, характеризующихся серьезными внутригосударственными и международными военно-политическими изменениями, возрастанием угрозы терроризма, активным и широким распространением новых высокотехнологичных средств коммуникации, перед руководством РФ стоит достаточно острая проблема пересмотра имеющихся подходов и доктрин по защите национальных интересов в глобальной сети. Новые вызовы и угрозы национальной безопасности обуславливают необходимость предотвращения появления конфронтации в виртуальном пространстве сети, появления интерактивного информационного оружия и возникновения сетевых информационных войн.

Во втором параграфе второй главы «Стратегии и технологии информационного противоборства в сети Интернет в контексте обеспечения информационной безопасности Российской Федерации» на примере югоосетинского конфликта августа 2008 г. анали-

зируются стратегии и технологии ведения сетевого информационного противоборства современной России.

Современный опыт информационного противоборства России свидетельствует о преобразовании политических технологий в сторону формирования виртуальной реальности информационной борьбы. Применяемые ныне политические Интернет-технологии России включают в себя как приемы достижения немедленного локального кратковременного результата, так и получение глубинного, глобального, длительного эффекта. Их комплексное использование во многом определяет эффективность политического управления, регулирования политических процессов и в значительной мере определяет устойчивость всего политического пространства.

Современные стратегии информационного противоборства России в сети Интернет представляют собой комплекс мероприятий, реализуемый по трем основным направлениям деятельности: информационное воздействие, информационное противодействие и стратегический политический анализ.

В целях информационного воздействия Россией применяются манипулятивные технологии, реализуемые при помощи наполнения политических текстов, размещенных в Интернет-пространстве, имеющих собственную систему стилистических, образных, семантических, синтаксических, риторических средств воздействия, технологиями виртуальной реальности.

Посредством контент-анализа политических текстов, размещенных в сети Интернет в период основного этапа грузино-югоосетинского конфликта (с 8 по 13 августа), доказывается, что наиболее действенными технологиями информационного воздействия, активно используемыми Россией в процессе ведения сетевого ИП, являются семантическое манипулирование, тактика речевого контраста «свои» - «чужие» и др.

Применяемые технологии способствуют достижению следующих целей манипулирования: эмоциональному воздействию через специальное доведение определенным образом подобранных негативных фактов; созданию положительного образа своего субъекта; отрицанию невыгодных фактов и явлений; формированию образа врага; позиционированию неправомочности действий противоборствующей стороны; утверждению однозначного образа действительности; созданию иллюзии объективности и достоверности информации.

Для реализации технических атак Россией используются различные механизмы воздействия на информационные сферы противоборствующего субъекта, создаются средства разрушения информации в Сети в целях получения несанкционированного доступа к закрытой

информации и ограничения (блокирования) доступа к собственным информационным web-ресурсам; проведение кибер-атаки против новостных, правительственных и других сайтов, что способствует потере противником потенциальной возможности влиять на умеренно настроенную аудиторию.

В целом применяемые в настоящее время Россией политические Интернет-технологии содействуют реализации основных целей информационного противоборства, позволяя создавать такую виртуальную среду, которая осознается как отражение реальной картины мира и дает возможность руководству РФ управлять обществом, формировать сознание. Однако для победы в информационной борьбе в Сети необходимо обеспечение более полномасштабного охвата целевой аудитории и достаточное количество информационных контактов с каждым из ее элементов. Практика ведения сетевого ИП показывает, что в настоящее время российские спецслужбы, политические институты, системы обороны, силовые министерства и ведомства не в полной мере готовы вести информационную борьбу на сетевом информационном поле: существующие на данный момент стратегии информационного противоборства России на практике оказываются малоэффективными против современных технологий виртуального пространства.

В третьем параграфе второй главы «**Повышение эффективности российской государственной системы информационного противоборства в сети Интернет: способы и технологии**» обуславливается необходимость совершенствования правовых механизмов регулирования общественных отношений, возникающих в виртуальном пространстве, и формулируются научные выводы, позволяющие содействовать дальнейшему развитию методов, способов и технологий повышения эффективности государственной правовой и информационно-технической баз обеспечения информационного противоборства в сети Интернет.

Современные угрозы личной, социальной, национальной безопасности, генерируемые несистемными акторами политического процесса, детерминируют разработку концепции кибербезопасности, суть которой заключается в минимизации рисков политической и социальной стабильности, исходящих из Интернет-пространства. Предложенная концепция должна быть реализована по следующим направлениям деятельности: формирование скоординированной политики РФ по отношению к виртуальному пространству; выработка государственных механизмов противодействия информационно-психологической агрессии в сети Интернет; организация интерактивной коммуникации с населением; постоянное взаимодействие с зарубежными государственными и негосударственными

медиаструктурами; развитие информационно-аналитических ресурсов выявление и предотвращения Интернет-угроз; проведение на постоянной основе мониторинга состояния виртуального сообщества России; координация деятельности негосударственных организаций в сфере управления Интернетом, внедрение действенных механизмов взаимодействия власти, общества и бизнес-структур в Сети; расширение международного сотрудничества в сфере организации противодействия акциям информационно-психологической агрессии в сети Интернет в условиях сетевого ИП.

В заключении подводятся итоги диссертационного исследования, формулируются основные выводы и практические рекомендации.

Российский сегмент Интернета постепенно превращается в арену социально-экономической борьбы, многоуровневого политического информационного противоборства. Специфическое свойство Интернета – возможность быстрого вбрасывания в глобальное информационное пространство как позитивных, так и негативных сведений – широко используется всеми политическими силами. Это обуславливает тот факт, что российские специалисты информационного противоборства в политической сфере начинают активно разрабатывать и применять стратегии информационного воздействия и противодействия.

Анализ действующей государственно-правовой системы регулирования глобальной сети Интернет России обуславливает необходимость решения ряда задач в области обеспечения кибербезопасности России, направленных на совершенствование правовых механизмов регулирования общественных отношений, возникающих в сети Интернет; разработку концепции кибербезопасности России и механизмов её реализации; федеральных целевых программ обеспечения информационной безопасности РФ в сети Интернет; достижение технологической независимости РФ в сфере информатизации, телекоммуникации и связи; разработку современных методов и средств защиты информации в сети Интернет, обеспечение безопасности сетевых информационных технологий; создание условий для активного развития российской инфраструктуры сети Интернет; участие России в деятельности глобальных информационных технологий, сетей и систем; создание оптимальной системы подготовки кадров в области информационных web-технологий, кибербезопасности, разработки антивирусного программного обеспечения и т.д.

В организационном аспекте формирования системы сетевого информационного противоборства России предлагается отказаться от концентрации усилий на «силовом», жестком контроле Интернет-контента, признать очевидность невозможности решения проблем в информационном пространстве виртуальной среды только за счет пе-

рекрытия (ликвидации) информационных каналов в условиях децентрализованной системы глобальной Сети; сосредоточиться на достижении эффективного обеспечения государственных интересов в виртуальном пространстве на основе комплексного подхода по всем направлениям информационного противоборства: политическому анализу, информационному воздействию и информационному противодействию.

III. Основные положения диссертационного исследования отражены в 10 публикациях автора общим объемом 3,7 п.л.:

Научные статьи, опубликованные в рецензируемых журналах, входящих в реестр ВАК РФ:

1. Соловьева Е.А. Управление Интернет-пространством в условиях информационного противоборства // Правовая политика и правовая жизнь. – 2010. – №1(38). – С. 150-155 (0,5 п.л.).

2. Соловьева Е.А. Информационное противоборство в сети Интернет // Социально-гуманитарные знания. – 2011. - № 7. – С. 263-268. (0,5 п.л.).

В международных изданиях:

3. Соловьева Е.А. Особенности информационного противостояния России и Грузии в сети Интернет // Политические и социальные процессы в Евразийском пространстве. В ожидании новой парадигмы: сб. статей // Сост. А.А. Саркисян / Отв. редактор А.А. Овсепян, В.М. Немчинов, Р.К. Бахсян, А.А. Филиппов. – Ереван: «Ноян Тапан». – 2010. – С.158-167 (0,7 п.л.).

В других изданиях:

4. Соловьева Е.А. Семантическое манипулирование как метод воздействия на общественное сознание, или информационная война между Россией и Грузией // Молодая наука – 2007: материалы региональной межвузовской научно-практической конференции студентов, аспирантов и молодых ученых. – Пятигорск: Изд-во ПГЛУ, 2007. – С. 21-25 (0,4 п.л.).

5. Соловьева Е.А. Проблемы информационного противостояния между Россией и Грузией // Мир на Северном Кавказе через языки, образование, культуру: материалы V Международного конгресса. – Пятигорск: Изд-во ПГЛУ, 2007. – С.60-62 (0,2 п.л.).

6. Соловьева Е.А. Роль СМИ в эволюции стереотипа восприятия грузинской нации российским обществом // Образ кавказца в центральной прессе: проблемы и решения: материалы Всероссийской на-

учно-практической конференции. – Махачкала: Изд-во ДГУ, 2008. - С. 36-37 (0,2 п.л.).

7. Соловьева Е.А. Проблема понятийного аппарата исследования конфликтов в информационном пространстве // Университетские чтения – 2009: материалы научно-методических чтений ПГЛУ. - Часть XII. - Пятигорск: Изд-во ПГЛУ, 2009. – С.51-55 (0,4 п.л.).

8. Соловьева Е.А. Интернет как социотехническое явление // Университетские чтения – 2010: материалы научно-методических чтений ПГЛУ. – Пятигорск: Изд-во ПГЛУ, 2010. – С. 117-120 (0,3 п.л.).

9. Соловьева Е.А. Интернет как инструмент сетевого воздействия на общественное сознание // Мир через языки, образование, культуру: Россия – Кавказ - мировое сообщество: материалы VI Международного конгресса. – Пятигорск: Изд-во ПГЛУ, 2010. – С. 87-89 (0,2 п.л.).

10. Соловьева Е.А. Концептуальные подходы к определению феномена информационного противоборства // Университетские чтения – 2011: материалы научно-методических чтений ПГЛУ. – Пятигорск: Изд-во ПГЛУ, 2011. – С.112-115 (0,3 п.л.).

Подписано в печать 21.11.2011.
Формат 60x84 1/16. Бумага офсетная. Печать офсетная.
Усл. печ.л. 1,2. Тираж 100 экз. Заказ 301.

ФГБОУ ВПО «Пятигорский государственный
лингвистический университет»
357532, Ставропольский край, г. Пятигорск, пр. Калинина, 9
Отпечатано в Центре информационных и образовательных тех-
нологий ФГБОУ ВПО «ПГЛУ»