На правах рукописи

**Колесов Олег Юрьевич**

# ТЕХНОЛОГИИ ФУНКЦИОНАЛЬНОГО ОБЕСПЕЧЕНИЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПОЛИТИКЕ: ОЦЕНКА ОТЕЧЕСТВЕННОГО И ЗАРУБЕЖНОГО ОПЫТА

Специальность 23.00.02 –
Политические институты, этнополитическая конфликтология,
национальные и политические процессы и технологии

Автореферат
диссертации на соискание
ученой степени кандидата политических наук

Нижний Новгород – 2007

Работа выполнена на кафедре политологии Нижегородского государственного университета им. Н.И. Лобачевского

Научный руководитель:

доктор политических наук, доцент
**Балуев Дмитрий Геннадьевич**

Официальные оппоненты:

доктор политических наук, доцент
**Рыхтик Михаил Иванович**
кандидат политических наук, доцент
**Марасов Михаил Геннадьевич**

Ведущая организация:

**Нижегородский государственный лингвистический университет им. Н.А. Добролюбова.**

Защита состоится « 22 » февраля 2007 г. в 13 часов на заседании Диссертационного совета Д-212.166.10 при Нижегородском государственном университете (603005, Нижний Новгород, ул. Ульянова, 2, ауд.315).

С диссертацией можно ознакомиться в фундаментальной библиотеке Нижегородского государственного университета по адресу: 603950 Нижний Новгород, пр. Гагарина, 23, корпус 1.

Автореферат разослан « 19 » января 2007 года.

Учёный секретарь
Диссертационного совета,
доктор исторических наук, профессор **Корнилов А.А.**

## I. Общая характеристика работы

**Актуальность темы** определяется научно-теоретической и практической значимостью проблем обеспечения информационной безопасности, их влиянием на общественное развитие.

В условиях глобализации мирового развития и информационной открытости национальных границ информация становится главным стратегическим фактором в международном соревновании за использование ее позитивных сторон и минимизацию негативных последствий. Результаты глобализационных изменений уже проявляются не только на технологическом уровне, но и на уровне социальных и духовных изменений общества, что ведет к формированию новой предметной области – информационной безопасности. Обеспечение информационной безопасности является одним из наиболее важных направлений международной деятельности технологически развитых стран мира. Вполне естественно, что в настоящее время в академических кругах и в среде лиц, принимающих политические решения, и Западе, и в России, преобладает желание найти новые подходы к проблемам обеспечения информационной безопасности на различных уровнях. При этом пока еще отсутствуют работоспособные и пригодные для практического анализа и выработки политики в области информационной безопасности концепции. Отсутствует и рассмотрение информационной безопасности как комплекса взаимосвязанных функциональных и институциональных систем.

Именно это обстоятельство и определяет **актуальность** темы настоящей диссертации, предполагающей рассмотрение проблем информационной безопасности России как комплекса взаимосвязанных систем.

**Степень разработанности проблематики исследования**

Характеризуя степень изученности проблемы системы политико-системного анализа информационной безопасности, следует отметить значительное количество работ, посвященных исследованию так называемой информационной теории.

В понимании сущности политической коммуникации автор опирался на работы зарубежных теоретиков: Г. Алмонда, М. Вебера, Д. Истона, Р.

Даля, К. Дойча, Ж.М. Коттрэ, Ч. Кули, А. Этциони, а также отечественных исследователей К.С. Гаджиева, А.А. Галкина, М.Н. Грачева, О.А. Колобова, В.В. Латынова, В.М.Сергеева, А.И. Соловьева, Е.Б. Шестопал.

Теоретическое осмысление проблем, возникших в связи с развитием новых информационных и телекоммуникационных технологий во второй половине XX века и легших в основу концепций информационного общества, представлено в работах таких исследователей, как Д. Белл, З. Бжезинский, Д.Гэлбрайт, М. Кастельс, Г.-М. Маклюэн, Ф. Махлап, М. Порат, Т. Стоуньер, Э. Тоффлер, А. Турен и др.. В отечественной науке, разрабатывающей проблемы информационного общества, значительное место принадлежит исследованиям: Р. А. Абдеева, В.М. Глушкова, И.С. Мелюхина, А.И. Ракитова, Г.Л. Смоляна, Д.С. Черешкина.

В исследовании трансформации информационного пространства на рубеже XX-XXI веков наиболее значимыми в понимании сути глобальных информационных процессов, происходящих в современном мире, стали взгляды В.Л. Иноземцева, О.А. Колобова, А.С. Панарина, В.П. Макарова, В.Р. Мединского, А.Ю Мельвиля. Наибольший вклад в развитие теории «информационного общества» как модификации концепций постиндустриального общества внесли Д.Белл, М. Порат, Й.Масуда. О.Тоффлер, Т. Стоуньер, Р.Катц, П.Дракер, М.Кастельс. Среди российских ученых следует отметить В.Л.Иноземцева, А.И.Ракитова, Р.Ф.Абдеева.

Проблемы информационных вызовов нового этапа политического развития анализируются в работах Е.Ю. Митрохиной, А.В. Манойло, И.Н. Панарина, А.И. Петренко, С.П. Расторгуева, Д.Б. Фролова.

Как и большинство работ по проблемам безопасности, основная масса исследований по собственно информационной безопасности посвящена ее военно-политическим и техническим аспектам. Известными западными специалистами в этой области, давшими рабочие определения «информационной безопасности», выделившими основные направления информационного противоборства, являются У.Швартау, М.Либики. Среди российских специалистов в области военно-политических аспектов информационной безопасности можно отметить В.П.Шерстюка, Цыгичко

В.Н., Г.Л.Смоляна и Д.С.Черешкина, Г.В.Емельянова и А.А.Стрельцова, И.Н.Панарина, О.А.Колобова и Ю.К. Меньшакова.

Таким образом, существует достаточно большое количество работ, посвященных проблемам роли информации в современном общественном развитии, информационной революции, информационному обществу, собственно информационной безопасности. Однако, оценивая их можно отметить, что пока еще отсутствуют когерентные и логически непротиворечивые подходы к самому определению понятия «информация», последствия информационной революции большей частью изучаются в их технологических приложениях, а не с точки зрения того, как они влияют на общество и управленческие процессы, концепция информационного общества в ее нынешнем виде вряд ли может быть теоретическим ориентиром при выработке конкретных управленческих решений в области информационной безопасности. Сама информационная безопасность в большинстве исследований сводится либо к защите информационной инфраструктуры (при этом игнорируется семантический уровень защиты), либо, напротив, чрезмерно расширено и не конкретно. Кроме того, не учитывается многоуровневость системы обеспечения информационной безопасности.

В этих условиях все большее количество исследователей призывает к развитию более всеобъемлющего и системного подхода к обеспечению информационной безопасности, принимающего во внимание широкие трактовки самого понятия информационная безопасность и многоуровневый характер системы обеспечения информационной безопасности. Данная работа призвана в какой то мере восполнить существующий пробел и предложить рассмотрение информационной безопасности как комплекса систем информационной безопасности и обеспечения информационной безопасности.

**Цель работы** - исследование проблем строительства и обеспечения эффективного функционирования систем обеспечения информационной безопасности национального и наднационального уровня. Для достижения этой цели представляется необходимым выполнить ряд **исследовательских задач**.

Во-первых, требуется детальное рассмотрение системы информационной безопасности как функциональной системы, определение основных понятий, составляющих сущность этого явления, выработка базовых определений пригодных для использования в политологическом анализе информационной безопасности.

Во-вторых, необходимо проанализировать опыт строительства и функционирования систем обеспечения информационной безопасности зарубежных стран.

В-третьих, должен быть проведен анализ опыта построения наднациональных систем обеспечения информационной безопасности.

В-четвертых, требуется рассмотреть существующую систему обеспечения информационной безопасности Российской Федерации и на этой основе предложить возможные пути ее совершенствования.

В соответствии с поставленными исследовательскими задачами находится и **структура** работы. Работа состоит из введения, трех глав и заключения. В первой главе рассматривается система информационной безопасности и ее компоненты. Вторая глава посвящена зарубежному опыту создания и обеспечения эффективного функционирования систем обеспечения информационной безопасности национального и наднационального уровня. Наконец в третьей главе выполняется политологический анализ системы обеспечения информационной безопасности Российской Федерации. В заключении изложены основные выводы исследования, сформулированы основные предложения по совершенствованию системы обеспечения информационной безопасности России.

**Объект и предмет исследования**

Объектом выступает информационная безопасность в различных ее проявлениях и на различных уровнях. Предметом исследования являются технологии функционального обеспечения систем информационной безопасности в политике в России и зарубежных странах.

**Эмпирическую базу исследования** составили: документы правительства России и зарубежных стран, аналитические материалы ведущих российских и зарубежных научных учреждений, крупнейших корпораций, занятых в сфере обеспечения информационной безопасности,

международные статистические данные, отечественные и зарубежные теоретические работы по проблемам национальной и информационной безопасности.

**Методологической основой диссертации** являются:

- общетеоретические политологические положения о системно-структурном подходе в познании сложных общественных реалий;
- аксиологический подход к изучению и творческому использованию богатейшего отечественного и зарубежного опыта обеспечения информационной безопасности;
- идеи взаимосвязанности и взаимообусловленности политических, социальных и идеологических факторов выработки управленческих решений в области обеспечения информационной безопасности;
- положения, выработанные в рамках социологии управления. Специфика примененного социологического подхода заключается, прежде всего, в том, что в центре внимания находятся механизмы взаимодействия людей, возникавшие в процессе их совместной профессиональной деятельности.
- комплексное рассмотрение исторических обстоятельств выработки и проведения политики в информационной безопасности.
- системный подход, предполагающий что информационная безопасность конкретного субъекта является результатом взаимодействия системы информационной безопасности и системы обеспечения информационной безопасности.

В диссертации использованы такие **методы исследования** как:

- метод восхождения от абстрактного к конкретному;
- принцип единства объективного и субъективного;
- анализ и синтез источников и материалов;
- метод кейз стади (исследование конкретного показательного случая);
- структурализация, позволяющая выделить в изучаемом явлении системообразующие факторы;
- различные приемы методологического анализа и классификации;
- систематизация и обобщение полученных выводов и результатов.

**Практическая значимость** исследования состоит в том, что:

- Его результаты могут быть использованы в процессе практической выработки управленческих решений в сфере обеспечения информационной безопасности.
- Теоретическое осмысление информационной безопасности позволит выработать практические рекомендации и более качественно решать важные народнохозяйственные задачи, связанные с развитием современной России.
- Результаты исследования будут использованы в учебном процессе в виде специальных курсов и включения отдельных тем в основные курсы для студентов-политологов.

**Основные положения диссертации, выносимые на защиту**

В качестве основных на защиту выносятся следующие положения**:**

1. Существуют т.н. «узкие» и «широкие» трактовки информационной безопасности. «Узкая» трактовка информационной безопасности понимает ее как защищенность собственных информационных ресурсов от возможных угроз. Согласно широкой трактовке информационная безопасность - защита собственных информационных систем от несанкционированного доступа при одновременном обеспечении поступления, а также независимого и эффективного анализа информации с возможностью в случае действий извне, направленных на достижение информационного превосходства, обнаружить “противника” и нанести сокрушающий удар по его информационным системам. Представляется, что подобное определение, несмотря на его кажущуюся громоздкость и описательный характер, вполне может использоваться для выработки стратегии информационной безопасности. При таком определении информационная безопасность будет означать и снятие информационной неопределенности относительно объективно и субъективно существующих потенциальных и реальных угроз. Широкая трактовка будет более полезной для выработки управленческих решений в области информационной безопасности на федеральном и международном уровне. Узкая трактовка является наилучшей для анализа информационной безопасности на местном уровне.

2. Зарубежный опыт функционального обеспечения систем информационной безопасности сильно варьируется в зависимости от

базовых политических установок той или иной страны. В США основной упор делается на связь информационной безопасности с безопасностью национальной. Цель политики информационной безопасности – в полной мере максимизировать возможности, которые информационная революция дает в военной области, оградив при этом свои информационные системы от атак потенциальных противников. Основные субъекты политики обеспечения информационной безопасности на национальном уровне – подразделения министерства обороны и силовые ведомства. Япония, как и большинство стран АТР, при обеспечении информационной безопасности в большей степени озабочена извлечением экономических благ из информационной революции. Система обеспечения информационной безопасности этой страны концентрируется на правоохранительных органах. В Западной Европе, начавшись с практически диаметрально противоположных направлений национальные и общеевропейская политика обеспечения информационной безопасности стремительно эволюционировали в направлении сближения основных принципов функционирования.

3. Национальные системы обеспечения информационной безопасности в условиях глобализации уже не могут в полной мере выполнять задачи, которые ставились при их создании.

4. В России само определение информационной безопасности до сих пор находится в стадии формирования. Очень часто толкование информационной безопасности (узкое или широкое) зависит от ведомственных интересов. Соответственно и структура системы обеспечения информационной безопасности пока еще не устоялась. Именно поэтому Россия находится в особо уязвимой позиции перед лицом разворачивающейся информационной революции. Однако перед некоторыми из ее потенциальных противников Россия все еще обладает преимуществом в информационной сфере. Использование этого преимущества вполне может сбалансировать относительную слабость в других сферах и служить важным дополнением к реализации влияния по дипломатическим каналам.

5. Для противостояния угрозам в информационной сфере и использования относительного преимущества над некоторыми из

потенциальных противников необходима четкая концепция информационной безопасности, опирающаяся на реально существующие общегосударственные, а не ведомственные интересы, и долгосрочная государственная политика по созданию ее материальной базы.

На основе проведенного анализа *автор предлагает ряд положений*, которые могут оказаться полезными при совершенствовании системы обеспечения информационной безопасности РФ, должны учитываться (на уровне учебных программ) при подготовке и переподготовке кадров и найти отражение в образовательных стандартах.

## Апробация результатов исследования

Результаты исследований нашли отражение в целом ряде публикаций в профессиональных и научных изданиях, выступлениях на российских и международных конференциях.

Основные положения диссертационного исследования были апробированы в ходе участия автора во Всероссийских и международных конференциях (Международной научной конференции «Национальная идентичность России и демографический кризис». Москва, ИНИОН РАН, 2006; Международной научно-практической конференции «Изменяющаяся Россия: проблемы безопасности и пограничной политики». Челябинск: Южно-Уральский государственный Университет - Челябинское отделение РАПН, октябрь 2006 года; «Дискурсология: методология, теория, практика». Челябинск: Институт философии и права УрО РАН, декабрь 2006 года), ряде региональных и межвузовских конференций и научно-практических семинаров. Результаты этих работ были отражены в ряде публикаций автора.

## II. Основное содержание работы

Во **введении** характеризуются актуальность, научная новизна, эмпирическая база, объект, предмет, цель и задачи, методология и методы, обоснованность и достоверность, практическая значимость, апробация,

структура, авторская концепция исследования, основные положения работы выносимые на защиту.

В **первой главе «**Информационная безопасность как социальное явление: разработка понятийного аппарата**»,** состоящей из четырех параграфов, определяется смысловое содержание основных используемых в работе терминологических образований. Рассматриваются различные подходы к определению информации и ее роли в политических процессах, существующие в политической науке подходы к информационной революции, а также дается теоретическое обоснование проблемы информационной безопасности.

В **первом параграфе главы, «**Информация как базовый концепт системы информационной безопасности**»**, рассматриваются различные подходы к самому понятию «информация». Особое внимание при этом уделяется структурному подходу, включающему в себя следующие уровни: идеальная надстройка, организационная структура, технологическая инфраструктура и лингвистическая субструктура.

Во **втором параграфе главы, «**Информационная революция и ее влияние на информационную безопасность**»**, основное внимание уделено феномену информационной революции. Отмечается, что в результате информационной революции в терминологический аппарат политических наук входят такие ассоциировавшиеся прежде с исследованиями в области коммуникаций и информации термины, как киберпространство, кибервласть, киберэлита, информационное общество. При этом информационная революция способствовала двум важнейшим тенденциям в развитии организаций: росту влияния малых групп и развитию сетевых форм организации. В настоящее время информационная деятельность осуществляется на операциональном, прагматическом уровне, через взаимодействие множества различных субъектов, решающих конкретные задачи, продиктованные состоянием корневых элементов общества: человека, природы, экологии и базовых систем жизнеобеспечения общества. При этом затрагиваются сферы экономической, политической, научной, гуманитарной, культурной, оборонной и иной социально значимой деятельности.

В **третьем параграфе главы, «**Взаимная соотносимость понятий «информационное общество» и «информационная сфера»», рассматривается то, какую эвристическую ценность имеет такое все более употребимое в общественных науках понятие, как «информационное общество». Анализируются различные подходы к определению информационного общества. Дается сравнительный анализ концепции информационного общества и информационной сферы.

**В четвертом параграфе «**Разработка понятий «информационная безопасность» и «угроза информационной безопасности» разрабатывается категориальный аппарат общей теории информационной безопасности. Выявляются существующие в отечественной и зарубежной политической науке подходы к базовым терминологическим конструкциям дисциплины. Проводится их классификация. На этой основе дается авторское определение информационной безопасности и классификация угроз информационной безопасности.

**Вторая глава** диссертационного исследования - «Зарубежный опыт управления системами обеспечения информационной безопасности**».** Рассмотренные в первой главе теоретические аспекты информационной безопасности создают основу для исследования практического применения данной концепции. На примере США, ряда стран Западной Европы и стран АТР автор попытался ответить на ряд вопросов, связанных с зарубежным опытом управления системами обеспечения информационной безопасности.

В **первом параграфе главы, «**Система обеспечения информационной безопасности в Северной Америке**»**, рассматриваются основные проблемы, с которыми столкнулись Соединенные Штаты. При этом отмечается, что является целесообразным рассмотрение Североамериканской системы обеспечения информационной безопасности как единого целого. Это связано с тем, что несмотря на не подвергаемый сомнению государственный суверенитет Канады, система обеспечения информационной безопасности этой страны весьма тесно интегрирована в систему США, основные стандарты в этой разделяются обеими странами, функционирование системы

обеспечения информационной безопасности обеспечивают те же специалисты. Вскрывается специфика системы информационной безопасности США. Проводится анализ нормативной базы функционирования системы обеспечения информационной безопасности. Рассматриваются конкретные политические решения, принятые для обеспечения эффективности функционирования этой системы. Отмечается, что в США основной упор делается на связь информационной безопасности с безопасностью национальной. Цель политики информационной безопасности – в полной мере максимизировать возможности, которые информационная революция дает в военной области, оградив при этом свои информационные системы от атак потенциальных противников. Система обеспечения информационной безопасности этой страны является наиболее развитой и многоуровневой, обеспеченной при этом соответствующей нормативной базой. Основные субъекты политики обеспечения информационной безопасности на национальном уровне – подразделения министерства обороны и силовые ведомства.

**Второй параграф главы - «**Опыт Японии**»,** рассматривает эту страну, как пример «бизнес-ориентированного подхода» к обеспечению информационной безопасности. Именно такой подход предопределяет спектр угроз информационной безопасности страны, и как следствие институциональные структуры, призванные обеспечить информационную безопасность. Япония, как и большинство стран АТР при обеспечении информационной безопасности в большей степени озабочена извлечением экономических благ из информационной революции. Информационная безопасность рассматривается, прежде всего, с точки зрения борьбы с компьютерными и экономическими преступлениями. Соответственно система обеспечения информационной безопасности этой страны концентрируется в правоохранительных органах.

**Третий параграф главы - «**Системы обеспечения информационной безопасности в Западной Европе**».** Диссертант рассматривает как национальные, так и наднациональные общеевропейские системы обеспечения информационной безопасности. В нем отмечается, что в Европе основное внимание уделяется социальной стороне нового этапа

технологической революции. Соответственно цель политики безопасности информации и информационных систем – защита целостности информации и гарантирование доступа к ней. Это является необходимым условием осуществления любой государственной политики. На государственном уровне информационная безопасность являлась прямым наследником тех времен, когда криптография была оружием, которым владело только государство, и которое использовалось для защиты собственной военной и дипломатической государственной информации и получения доступа к подобной информации других государств. Начавшись с практически диаметрально противоположных направлений национальные и общеевропейская политика обеспечения информационной безопасности стремительно эволюционировали в направлении друг друга. Изначально национальные политики основывались на главенстве разведывательной работы и криптографической защите данных. К настоящему времени они эволюционировали к большей открытости признанию необходимости обмена информацией и проведения совместных исследований в области обеспечения информационной безопасности. ЕС, который не имел опыта в области разведки, вынужден обращаться к политическим инструментам, которые до этого использовались лишь отдельными государствами.

**В четвертом параграфе** автор обращается к опыту ООН по строительству наднациональной системы обеспечения информационной безопасности. Обозначаются основные контуры этой системы. Дается оценка ее нынешней и потенциальной эффективности. Отмечается, что национальные системы обеспечения информационной безопасности в связи с глобализацией уже не могут в полной мере выполнять задачи, которые ставились при их создании. ООН в этих условиях в перспективе может стать механизмом обеспечения информационной безопасности на глобальном уровне.

**В третьей главе - «**Система обеспечения информационной безопасности в РФ**» -** проводится комплексное рассмотрение системы обеспечения информационной безопасности РФ, позволяющего прийти к значимым в научном и практическом плане выводам. Для этого последовательно решаются следующие задачи:

- Анализируется специфика российского подхода к обеспечению информационной безопасности, который во многих аспектах отличается от американского или западно-европейского.
- На этой основе рассматривается существующая нормативная база функционирования системы обеспечения информационной безопасности, насколько она соответствует особенностям российского подхода, какие ее составные части требуют совершенствования, предлагаются основные пути подобного совершенствования.
- Исследуется структура и функциональные особенности существующей системы обеспечения информационной безопасности РФ.

При этом особый интерес для автора представляли российские особенности, которые не позволяют ограничиться простым копированием зарубежного опыта и требуют достаточно серьезного учета страновой специфики.

В **первом параграфе - «**Специфика российского подхода к обеспечению информационной безопасности**»** - исследуются различные подходы к решению проблем информационной безопасности, существующие в академической среде, сообществе лиц, принимающих политические решения на различных уровнях, а также в бизнес сообществе. Дается анализ возможных угроз информационной безопасности страны.

Во **втором параграфе - «**Нормативная база функционирования системы обеспечения информационной безопасности**»** - автор анализирует как законодательную базу, так и ее практическое применение. При этом дается анализ не только федерального законодательства, но и региональных и ведомственных нормотворческих инициатив.

В **третьем параграфе - «**Структура и функциональные особенности системы обеспечения информационной безопасности РФ**»** - рассматривается правовые, организационно-технические и экономические методы обеспечения информационной безопасности. Дается классификация объектов и субъектов системы обеспечения информационной безопасности. Обозначается структура системы

обеспечения информационной безопасности страны. Выделяются функциональные особенности этой системы. Отмечается, что, несмотря на ряд очень серьезных проблем с материальной базой информационной безопасности России, страна пока еще обладает рядом ресурсов, которые при продуманной государственной политике могут обеспечить возрождение (а точнее - создание) этой базы. При отсутствии же этой политики существующая информационная база может стать не базой для информационной безопасности, а базой для информационной уязвимости.

Делается вывод о том, что важнейшее значение имеет активное сотрудничество государства с частными компаниями, например, по проблемам информационной безопасности. Очевидно, что для противостояния угрозам в информационной сфере и использования относительного преимущества над некоторыми из потенциальных противников необходима четкая концепция информационной безопасности, опирающаяся на реально существующие общегосударственные, а не ведомственные интересы, и долгосрочная государственная политика по созданию ее материальной базы.

В **заключении** диссертации выделены основные тенденции развития систем обеспечения информационной безопасности России и зарубежных стран, изложены авторские выводы, обозначена область их возможного применения и направления дальнейших исследований. Последовательно решая поставленные исследовательские задачи, автор пришел к следующим выводам.

*Во-первых*, традиционный взгляд на информацию как на процесс ее обработки является недостаточным. Аналитические конструкции, которые включают в себя также структурный взгляд, видятся более оправданными и показывают, что информация выступает гораздо более широкой и глубокой концепцией, чем принято думать. Взгляд, связанный с обработкой, обращает особое внимание на технологическую инфраструктуру. В результате этого часто считается, что организации могут быть усилены за счет использования новой информационной и коммуникационной технологии без изменения структуры самой организации. Более того, если какая-то организация сопротивляется

изменениям, в ней, скорее всего, будет преобладать взгляд на информацию, как на процесс обработки. Структурный взгляд, напротив, обращает особое внимание на ценности, цели и принципы организации. Структурный взгляд связан с той частью информационной революции, которая оперирует "знанием", а не "данными", поскольку вовсе не данные определяют природу структуры. Сегодня необходимо, чтобы стратегии в области информационной безопасности развивали структурный подход, идущий параллельно с подходом, основывающимся на процессе обработки информации.

*Во-вторых*, информационная революция способствовала двум важнейшим тенденциям в развитии организаций: росту влияния малых групп и развитию сетевых форм организации. Иерархии при этом не являются отжившими структурами. Однако они должны приспосабливаться к новым условиям. Необходимо сочетать иерархическую и сетевую форму организации, что само по себе является сложнейшей задачей. В одних областях сетевая организация может сменить иерархическую. В других могут появиться новые виды иерархий, которые лучше приспособлены для информационной эпохи. В третьих областях наилучшим решением могут являться гибриды двух форм организации. Все это отчетливо проявляется и на региональном уровне управления системой информационной безопасности.

*В-третьих*, видение конфликта информационной эпохи и, соответственно, информационной безопасности, должно включать в себя четыре составные части: концептуальные, организационные, доктринальные основы и соответствующую стратегию.

Концептуальная основа должна включать в себя широкий взгляд на информацию, о котором пишется в первой главе работы.

Организационный взгляд обращает особое внимание на основное последствие информационной революции — развитие сетевых форм организации. Информационная революция усиливает малые формы, которые лучше приспособлены для того, чтобы воспользоваться преимуществами сетевой формы организации.

Подводя итог существующим взглядам на информационное общество и его роль в исследовании проблем безопасности, можно констатировать,

что хотя термин "информационное общество" и имеет некоторую эвристическую ценность для исследования черт современного мира, пока еще он слишком неточен и неопределенен. Пока еще отсутствует общепринятый критерий, выделяющий принципиальную новизну этого общества и его отличие от предыдущих. Большинство этих определений оперирует с количественными характеристиками ("больше информации"), а не качественными показателями.

*В-четвертых*, любая целостная концепция информационной безопасности должна основываться на ясном и четком определении самого термина “информационная безопасность”. При этом, на наш взгляд, является неуместным как используемое в ряде исследований технократическое сведение информационной безопасности к безопасности компьютерных сетей, так и неоправданно широкая трактовка, включающая защиту культурных норм и устоявшихся поведенческих стереотипов или борьбу за чистоту языка (которое свойственно, например, нынешней Доктрине информационной безопасности). При этом подобная концепция должна основываться на четком представлении об угрозах информационной безопасности. Именно понятие «угроза информационной безопасности» является ключевым как для теоретического осмысления информационной безопасности, так и для выработки и проведения политики в этой области. Оно должно быть отправной точкой при выработке любой концепции информационной безопасности. Из всего многообразия существующих подходов к определению понятия «угроза информационной безопасности» наиболее ценным является определение, согласно которому, угроза - наиболее конкретная и непосредственная форма вероятности нанесения вреда социуму, совокупность условий и факторов, создающих опасность интересам граждан, общества и государства, а также национальным ценностям и национальному образу жизни в информационной сфере. Несмотря на господство как в научной среде, так и среди лиц, принимающих решения, классификации угроз безопасности по критерию источника угрозы (внутренняя и внешняя), в условиях глобализации, интернационализации и перехода к информационному обществу, гораздо более продуктивным может быть взятие за основу таких критериев как сферы происхождения и реализации

угроз, уровень их актуализации, являются ли угрозы информационной безопасности симметричными или асимметричными. Именно они позволяют выработать стратегии эффективного противодействия новым угрозам в изменившемся стратегическом окружении.

Существует множество трактовок понятия информационная безопасность. На одном конце спектра находится «узкая» трактовка информационной безопасности, которая понимает ее как защищенность собственных информационных ресурсов от возможных угроз. Представляется, что необходимо более широкое понимание информационной безопасности, согласно которой это - защита собственных информационных систем от несанкционированного доступа при одновременном обеспечении поступления, а также независимого и эффективного анализа информации с возможностью в случае действий извне, направленных на достижение информационного превосходства, обнаружить “противника” и нанести сокрушающий удар по его информационным системам. Представляется, что подобное определение, несмотря на его кажущуюся громоздкость и описательный характер, вполне может использоваться для выработки стратегии информационной безопасности. При таком определении информационная безопасность будет означать и снятие информационной неопределенности относительно объективно и субъективно существующих потенциальных и реальных угроз.

*В-пятых*, зарубежный опыт функционального обеспечения систем информационной безопасности сильно варьируется в зависимости от базовых политических установок той или иной страны. В США основной упор делается на связь информационной безопасности с безопасностью национальной.

В Японии, как и в большинстве стран АТР, система обеспечения информационной безопасности концентрируется на правоохранительных органах.

В Западной Европе национальные политики эволюционировали к большей открытости признанию необходимости обмена информацией и проведения совместных исследований в области обеспечения

информационной безопасности. ЕС, который не имел опыта в области разведки, вынужден обращаться к политическим инструментам, которые до этого использовались лишь отдельными государствами.

*В-шестых*, в целом можно отметить, что национальные системы обеспечения информационной безопасности в связи с глобализацией уже не могут в полной мере выполнять задачи, которые ставились при их создании. ООН в этих условиях начинает становиться механизмом обеспечения информационной безопасности на глобальном уровне при одновременном усилении роли ЕС в обеспечении информационной безопасности на уровне региональном.

*В-седьмых*, подводя итог анализу особенностей отечественного опыта функционального обеспечения систем информационной безопасности в политике можно отметить, что само определение информационной безопасности до сих пор находится в стадии формирования. Очень часто толкование информационной безопасности (узкое или широкое) зависит от ведомственных интересов. Соответственно и структура системы обеспечения информационной безопасности пока еще не устоялась. Законодательная база, для функционирования этой системы, несмотря на свою обширность, имеет значительные лакуны.

Именно поэтому Россия находится в особо уязвимой позиции перед лицом разворачивающейся информационной революции. С одной стороны, Россия в ближайшем будущем, возможно, будет вынуждена противостоять угрозам с юга и востока со стороны государств, самопровозглашенных квазигосударственных образований и негосударственных объединений, многие из которых сами не могут быть целями для информационных атак. С другой стороны, они вполне могут использовать информационные технологии для нанесения достаточно ощутимого урона России, информационная система которой, хотя и не является достаточно развитой для противостояния передовым государствам, жизненно необходима для функционирования экономики страны и для успешного ведения ей боевых действий.

Однако Россия обладает и рядом преимуществ в информационной сфере, использование которых вполне может сбалансировать

относительную слабость в других сферах и служить важным дополнением к влиянию по дипломатическим каналам.

*В-восьмых*, информатизация и эффективное функционирование системы обеспечения информационной безопасности тесно связаны с наукой и образованием, что обусловливает решающую роль и полную ответственность государства за то место, которое занимает страна в мировой технологической гонке. Важнейшее значение имеет активное сотрудничество государства с частными компаниями, например, по проблемам информационной безопасности. Очевидно, что для противостояния угрозам в информационной сфере и использования относительного преимущества над некоторыми из потенциальных противников России необходима хорошо продуманная концепция информационной безопасности, опирающаяся на реально существующие общегосударственные, а не ведомственные интересы, предлагающая асимметричные ответы на асимметричные угрозы, и долгосрочная государственная политика по созданию ее материальной базы.

К **областям конкретного применения результатов исследования** автор относит: политологию, в особенности ее раздел, связанный с политическими процессами и институтами, теорию международных отношений, всеобщую историю, конфликтологию. Научные и научно-политические итоги диссертации могут быть использованы практическими государственными органами, занимающимися вопросами безопасности и внешней политики (прежде всего Советом Безопасности РФ, ФСБ, СВР и МИД РФ, соответствующими подразделениями Министерства обороны РФ, их высшими учебными и научно-исследовательскими структурами), а также общественными организациями, заинтересованными в проблемах обеспечения информационной безопасности. Результаты исследования могут быть полезны разработке новых редакций Концепции национальной безопасности РФ и Концепции внешней политики РФ.

**Основные направления дальнейших исследований**. Перспективы изучения функциональных особенностей систем обеспечения информационной безопасности определяются той особой значимостью, которая имеет отношение к стратегическим интересам Российского государства, проявляющимся в самых различных аспектах политической

жизни общества и настоятельно требующим адекватной оценки учеными, общественными и политическими деятелями, а, главное, лицами, принимающими политические решения.

Одним из важнейших направлений познания проблем информационной безопасности представляется комплексный анализ международно-политического измерения проблемы, создание и операционализация концепции информационной безопасности, отражающей отечественный и зарубежный опыт функционального обеспечения систем информационной безопасности в политике, исследование новых угроз информационной безопасности.

**Основные положения** диссертации отражены в следующих публикациях:

1.) Публикации в изданиях, рекомендованных ВАК РФ

1) Колесов, О.Ю. Информационная безопасность как политическое явление: разработка понятийного аппарата/ О.Ю.Колесов // Вестник Нижегородского государственного университета им. Н.И Лобачевского. Серия «Международные отношения. Политология. Регионоведение».- Н.Новгород: Изд-во ННГУ им.Н.И Лобачевского, 2006.- №3 (4). (0,4 п.л)
2) Колесов, О.Ю., Ведяскин, М.В. К вопросу о месте информационно-психологического воздействия в современном политическом процессе/ О.Ю.Колесов, М.В.Ведяскин // Вестник Нижегородского государственного университета им. Н.И Лобачевского. Серия «Международные отношения. Политология. Регионоведение».-

Н.Новгород: Изд-во ННГУ им.Н.И Лобачевского, 2006.- №3 (4). - 0,5 п.л (авторский вклад 0,3 п.л.)

2.) Научные публикации

3) Колесов, О.Ю. Европейский опыт строительства наднациональной системы обеспечения информационной безопасности/О.Ю.Колесов // Вопросы гуманитарных наук – 2006. - № 6. (0,3 п.л.)
4) Колесов, О.Ю. Исследования информационной безопасности с позиций политического дискурса/О.Ю.Колесов // «Дискурсология: методология, теория, практика». Челябинск: Институт философии и права УрО РАН - Уральский государственный университет - Издательский Дом «Дискурс-Пи», 2006. (0,3 п.л.)
5) Колесов, О.Ю., Балуев Д.Г. Региональный уровень функционирования системы обеспечения информационной безопасности/О.Ю.Колесов, Д.Г.Балуев // «Изменяющаяся Россия: проблемы безопасности и пограничной политики». Челябинск: Южно-Уральский государственный Университет - Челябинское отделение РАПН, 2006. - 0,4 п.л (авторский вклад 0,3 п.л.)
6) Колесов, О.Ю. Разработка вопросов информационной безопасности в трудах нижегородской международно-политической школы / О.Ю.Колесов// Нижегородский журнал международных исследований. Осень-Зима, 2006. (0,2п.л)
7) Колесов, О.Ю., Балуев, Д.Г. Глобализация и ее последствия для места России в мире/О.Ю.Колесов, Д.Г.Балуев // «Национальная идентичность России и демографический кризис». Москва: ИНИОН РАН, 2006. - 0,6 п.л (авторский вклад 0,4 п.л.)