На правах рукописи

Судоргин Олег Анатольевич

ИМПЕРАТИВЫ И ПРИОРИТЕТЫ ПОЛИТИКИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ

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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата политических наук

Москва – 2005

Работа выполнена на кафедре социальных наук и государственного управления Московского государственного областного университета

Научный руководитель – Пирогов Александр Иванович
доктор философских наук, профессор

Официальные оппоненты: – Ницевич Виктор Францевич
доктор политических наук, доцент

– Белозеров Василий Клавдиевич
кандидат политических наук

Ведущая организация – Московский городской университет управления Правительства Москвы

Защита состоится "24" июня 2005 г. в 15 часов на заседании диссертационного совета К-212.141.01 по политическим наукам в Московском государственном техническом университете им. Н.Э. Баумана по адресу: г. Москва, ул. 2-я Бауманская, д. 5.

С диссертацией можно ознакомиться в библиотеке Московского государственного технического университета им. Н. Э. Баумана по адресу: г. Москва, ул. 2-я Бауманская, д. 5.

Автореферат разослан "16" мая 2005 года.

Ученый секретарь
диссертационного совета
кандидат философских наук, доцент С.А. Власов

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИССЕРТАЦИИ

На современном этапе борьбы государств за сферы влияния акцент с явного применения силы все заметнее смещается на использование более гибких средств, основными из которых является контроль и управление информационными ресурсами государств. Для достижения этих целей в условиях возрастающей насыщенности информационными и управляющими средствами, в том числе и иностранного производства, может быть использовано высокоэффективное и скрытное проникновение в программное обеспечение государственных информационных и управляющих систем России.

Стремительное развитие технологий работы с информацией в развитых странах обуславливает формирование стратегий "информационной войны", главной целью которой является информация, овладение ею или изменение в своих интересах. Очевидным становится факт, что информационные технологии играют исключительно важную роль не только в обеспечении национальной безопасности, но и в развитии личности, общества и государства в современных условиях.

Актуальность темы диссертационного исследования обусловлена следующими положениями.

Во-первых, информационная безопасность занимает одно из ключевых мест в системе обеспечения жизненно важных интересов всех стран, и, безусловно, Российской Федерации. Это в первую очередь обусловлено насущной потребностью создания развитой информационной среды общества. Но именно через информационную среду зачастую осуществляются угрозы национальной безопасности в разных сферах деятельности личности, общества и государства. В современных условия возникла потребность в теоретическом осмыслении проблемы информатизации Российской Федерации через призму ее информационной безопасности.

Во-вторых, особой ролью информации в функционировании всех сфер общественной жизни. Так, в политической сфере именно информационные факторы приобретают все большее значение. В традиционном противостоянии политических соперников растет удельный вес и значимость информационного воздействия. Экономический потенциал государства тоже все больше определяется объемом информационных ресурсов и уровнем развития информационной инфраструктуры. В то же время растет потенциальная уязвимость экономических структур от недостоверности или запаздывания информации. В военной сфере исход вооруженной борьбы зачастую прямо зависит от качества добываемой информации и уровня развития информационных технологий, на которых основываются системы разведки, радиоэлектронной борьбы,

управления войсками и высокоточным оружием. Особое место занимает информация в обеспечении и осуществлении внешнеполитической деятельности государства. Без создания условий формирования достоверной, полной и своевременной информации для принятия внешнеполитических решений и предотвращения незаконного использования актуальной информации о внешнеполитической деятельности, той информации, которая обеспечивает приоритеты России на внешнеполитической арене, Россия не сможет играть достойную роль в мировом обществе. Поэтому существует необходимость дальнейшего углубленного познания информационной безопасности как объекта политики.

В-третьих, поскольку информационная безопасность является неотъемлемой частью политической, экономической, оборонной и других составляющих сфер жизни и деятельности личности, общества и государства в России и, в то же время она представляет собой самостоятельную область безопасности, призванной обеспечить защиту информации, требуется научное обоснование и разработка императивов политики обеспечения информационной безопасности Российской Федерации и возможностей использования ее теоретических конструкций в практических целях.

В-четвертых, интеграция России в мировое информационное пространство сопровождается все большим ростом открытия российского общества. Россия встраивается в уже существующее информационное пространство как планетарного, так и регионального масштабов, в которых существуют определенные "правила игры" и стандарты безопасности, а также используются информационные технологии. Процесс рационального сопряжения формирующегося информационного пространства и изменяющегося международного пространства требует научного обоснования приоритетов политической деятельности социальных и институциональных субъектов в решении задач информационной безопасности России.

В-пятых, технологизация работы с информацией, становление информационного общества в условиях упрочения демократии в нашем отечестве и усиление роли гуманизма в общественных отношениях требует новых решений в области обеспечения информационной безопасности личности, общества и государства в России.

Важно подчеркнуть, что проблеме обеспечения информационной безопасности России постоянно уделяется особое внимание со стороны ученых и практиков. Однако работ, напрямую исследующих политику обеспечения информационной безопасности Российской Федерации, тем более ее императивы и приоритеты, остается недостаточно. В силу этого выбранная тему призвана восполнить определенный пробел научного знания в области информационной безопасности и его применения на практике.

Степень научной разработанности темы. Проблема информационной безопасности является предметом рассмотрения многих ученых, специальных институтов и центров, представляющих различные научные отрасли знания, при чем, как гуманитарные, так и технические. В России внимание политологов к этой проблеме было привлечено недавно, точнее – в начале 90-х гг. XX в. Однако в отечественной науке в целом накоплен потенциал для углубленного исследования проблемы информационной безопасности.

Вместе с тем, общественный интерес к информационной проблематике наиболее полно отражается в научных трудах зарубежных ученых. В их работах раскрываются теоретические и методологические основы трансформации западных обществ в новую информационную стадию своего развития, рассматриваются социальные, технические, политические, экономические и иные предпосылки этого процесса, дается детальная характеристика связанных с этим изменений во всех областях жизни и деятельности общества, обосновываются возможные негативные влияния информационной революции на человека, социальные группы и общности людей. Значимость исследований таких авторов, как Д. Белл, Зб. Бжезинский, Э. Брэнском, Дж. Вакка, Э. Дайсон, М. Кастельс, И. Масуда, А. Минка, Дж. Нейсбит, С. Нора, Э. Паркер, О. Тоффлер, Х. Шпиннер и др. представляется возможным объединить в первую группу[1].

[1] Bell D. The coming of post-industrial society. A venture in social forecasting. N.Y.: Basic Books, Inc., 1973; Bell D. The Social framework of the information society. Oxford, 1980; Brzezinsky Z. Between two ages. America's role in the technotronic era. N.Y.: The Viking Press, 1970; Collins L. Grand strategy,princi ples and practice. Annapolis,Mariland,1993; Gershuny T. After industrial society? L.,1978; Masuda Y. The information society as postindustrial society. Wash.: World Future Soc., 1983; Naisbitt T. Megatrends: The new directions transforming our lives. N.Y., 1982; Branscomb A. Law and culture in the information society // Information soc. N.Y., 1986. Vol. 4; Nelson B.K. Applying the princi ples of war in information operations // Military Review. 1998; Nora S., Minc A. The computerization of society: A report to the President of France. Cambridge, L., 1980; Russet B. Controlling the sword. 1990. Vol. X.; Edelstein A. Total propaganda. From mass culture to popular culture. Mahway – London, 1997; Spinner H.F. Die Informationsgesellschaft - mehr Chaos als Mythos // Technologis: Das Vorstellbaren, das Wunschbare, das Machbare. Weinheim: Basel, 1986; Toffler A. Future shock. Canada, 1971; Toffler A. Power shift. N.Y., 1992; Toffler A, Toffler H. War and anti-War survival at the down 21st century. Canada, 1993; Toffler A. The third wave. N.Y., 1980;

Вторую группу источников составляют работы отечественных авторов, которые исследуют возрастание роли информации в современном обществе. В них раскрываются характеристика информатизации, как объективной закономерности развития общества, проблемы становление информационной цивилизации, даются прогнозы о развитии информационной цивилизации и исследуются технические и гуманитарные факторы этого процесса[1].

Vacca G. Die telematik-demokratische Informations Gesellschaft oder Herrschaft der Banalitot: Der Sozialismus an der Schwellezum 21. B., 1985; Дайсон Э. Жизнь в эпоху интернета. Release 2.0. Пер. с англ. / Под ред. А. В. Евтюшкина и Ю. А. Кузьмина. М., 1998; Кастельс М. Информационная эпоха: экономика, общество и культура. Пер. с англ. / Под ред. О.И.Шкаратана. М., 2000; Уэбстер Ф. Теории информационного общества /Пер. с англ. М.В. Арапова, Н.В. Малыхиной. Под ред. Е.Л. Вартановой. – М.: Аспект Пресс, 2004.

[1] Абдеев Р.Ф. Философия информационной цивилизации. – М.: Владос, 1994; Афанасьев В.Г. Социальная информация. – М.: Наука, 1994; Глушков В.М. Основы безбумажной информатики. – М., 1987; Ершова Е.В. Международный обмен информацией: правовые аспекты. – М.: Междунар. отношения, 1988; Коган В.З. Человек в потоке информации. – Новосибирск: Наука, 1981; Лекторский В.А. Возможна ли интеграция естественных наук и наук о человеке? //Вопросы философии. – 2004. – № 3; Моисеев Н.Н. Информационное общество как этап новейшей истории // Свободная мысль. – 1996. – №1; Моргунов Е.Б. Человеческий фактор в компьютерных системах. – М.: Тривола, 1994; Новая постиндустриальная волна на Западе: Антология /Под ред. В.Л. Иноземцева. – М., 1999; Пирогов А.И. Информатизация российского общества и укрепление обороноспособности страны. Дис. ... д-ра филос. наук. – М.: ВУ, 1996; Поздняков А.И. Информатика и ее роль в укреплении обороноспособности страны: Дис. ... д-ра филос. наук. – М.: ВАГШ, 1991; Пусько В.С. Научно-техническая политика социалистического государства: сущность, содержание, роль в укреплении экономической мощи и материально-технической базы обороны страны: Дис. ... д-ра филос. наук. – М.: ВПА, 1986; Ракитов А.И. Компьютерная революция и информатизация общества. – М., 1990; Он же. Россия в глобальном информационном процессе и региональная информационная политика. – М., 1994; Соколова И.В. Социальная информатика и социология: проблемы и перспективы взаимосвязи. – М.: МГСУ, 1999; Тихомиров М.Ю. Информационное общество: философские проблемы управления наукой и образованием. – М., 1999; Трансформации в современной цивилизации: постиндустриальное и постэкономическое общество: (Материалы круглого стола) //Вопросы философии. – 2000. – № 1;

Третью группу источников составляют труды, в которых исследуются методологические, сущностные и содержательные основы информационной безопасности. Среди таких работ особенно ценными оказались труды Н.И. Бусленко, С.Н. Гриняева, В.Д. Цыганкова, В.Н. Лопатина, М.Н. Чеснокова, А.И. Позднякова, Е.А. Беляева[1].

Четвертую группу составили источники, связанные с осмыслением политики обеспечения информационной безопасности Российской Федерации[2].

Урсул А.Д. Информатизация общества: Введение в социальную информатику. – М., 1990; Он же. Переход России к устойчивому развитию. Ноосферная стратегия. – М., 1998; Щедровицкий Г.П. Интеллект и коммуникация // Вопросы философии. – 2004. – № 3; Юзвишин И.И. Информациология или закономерности информационных процессов и технологий в микро- и макромирах Вселенной. – М.: Радио и связь, 1996; Яковец Ю.В. Формирование постиндустриальной парадигмы // Вопросы философии. – 1997. – № 1 и др.

[1] Андрианов Д.А. Политическая компонента информационной безопасности российского общества: Автореферат дисс... кандид. полит. наук. – М., 2002; Беляев Е.А. Информационная безопасность как глобальная проблема / Международная конференция «Глобальные проблемы как источник чрезвычайных ситуаций» / Доклады и выступления. / Под ред. Воробьева Ю.Л. – М.: УРСС, 2000; Бусленко Н.И. Политико-правовые основы обеспечения информационной безопасности Российской Федерации в условиях демократических реформ: Дис. ... д-ра полит. наук. – Ростов н/Д, 2003; Лукашин А.Н., Ефимов А.И. Проблема безопасности компьютерной инфосферы стратегических оборонных систем // Военная мысль. – 1995. – № 5; Национальная безопасность: информационная составляющая / Под общ. ред. В.В. Еременко. – М.: МОСУ, 2000; Панарин А.С. Глобальное информационное общество: вызовы и ответы // Власть. – 2001. – № 1; Поздняков А.И. Информационная безопасность личности, общества и государства // Военная мысль. – 1993. – № 10; Филимонов А.Ф. О разработке в США системы мер по защите национальной информационной структуры // Информационное общество. – 1997. – № 1; Цыганков В.Д., Лопатин В.Н. Психотронное оружие и безопасность России. – М.: СИНТЕГ, 1999; Чесноков М.Н. О защите информации. Пушкин, 1995 и др.

[2] Аносов В. Д., Стрельцов А. А., Ухлинов Л. М. О федеральной программе выявления и пресечения преступлений в сфере компьютерной информации // Проблемы информационной безопасности. – 1999. – № 1; Гриняев С.Н. Интеллектуальное противодействие информационному оружию. – М.: СИНТЕГ, 1999; Информационные вызовы национальной и

В пятую группу вошли источники, в которых раскрываются особенности и отдельные стороны обеспечения информационной безопасности России[1].

Несмотря на то, что существует множество научных трудов по проблемам информационной безопасности, следует подчеркнуть тот факт, что их содержание носит с одной стороны дискуссионный характер, а с другой – политика ее обеспечения представляется в фрагментарном виде.

Таким образом, недостаточная научная разработанность проблемы, фрагментарный характер и ее огромная теоретическая и практическая значимость обусловили выбор темы диссертационного исследования.

Объектом исследования является информационная безопасность Российской Федерации. Предметом выступает политика обеспечения информационной безопасности России.

Цель исследования состоит в решении важной научной задачи заключающейся в определении и обосновании императивов и приоритетов политики обеспечения информационной безопасности Российской Федерации.

Общий замысел и поставленная цель определили необходимость сформулировать и решить исследовательские задачи. А именно:

– осуществить анализ информационной безопасности как явления и объекта политики;

– уточнить сущность, содержание и функции политики обеспечения информационной безопасности;

международной безопасности /Под общ. ред. А.В. Федорова, В.Н.Цыгичко. – М.: ПИР-Центр, 2001; Ницевич В.Ф. Информационный фактор национальной безопасности. – Орел: «Вариант – В», 1999; Почепцов Г.Г. Информационные войны. – М.: «Рефл-бук»; К.: «Ваклер», 2000; Правовые основы защиты информации: Учебн. пособие. – Барнаул: АГТУ, 2000; Цыганков В.Д., Лопатин В.Н. Психотронное оружие и безопасность России. – М.: СИНТЕГ, 1999; Чертополох А.А., Костин А.В. Информационный фактор в военной политике государства. – М.: ВУ, 2000 и др.

[1] Концепция совершенствования правового обеспечения информационной безопасности Российской Федерации. Проект // Информационное общество. – 1999. – № 6; Кубышкин А.В. Международно-правовые проблемы обеспечения информационной безопасности государства: Дисс. ... канд. юрид. наук. – М.: МГЮА, 2002; Ницевич В.Ф. Императивы и приоритеты военно-информационной политики государства: Дисс. ... докт. полит. наук. – М.: ВУ, 2002; Стрельцов А.А. Направления совершенствования правового обеспечения информационной безопасности Российской Федерации //Информационное общество. – 1999. – № 6. – С. 15 – 20 и др.

– выявить и раскрыть содержание основных императивов политики обеспечения информационной безопасности России;

– определить механизм реализации императивов отечественной политики обеспечения информационной безопасности;

– обосновать приоритеты политики обеспечения информационной безопасности России;

– разработать первостепенные меры обеспечения информационной безопасности Российской Федерации.

Теоретико-методологическую основу исследования составляют положения общей теории политики, теории информации, информационной безопасности, теории управления применительно к предмету диссертации; принципы политики информационной безопасности, понятия политологии, информатики, кибернетики; системно-функциональный, институциональный, деятельностный и логический подходы; общенаучные методы познания – анализ, синтез, абстрагирования, аналогии, теоретического обобщения и др.

Значительную роль в расширении представления диссертанта об исследуемой проблеме сыграли материалы периодической печати, отражающие влияние информации, новых информационных технологий на состояние и процесс обеспечения безопасности России, а также личные впечатления от посещения выставок зарубежной и отечественной информационно-коммуникационной, вычислительной техники, современных информационных технологий, средств защиты информации, практический опыт работы автора в Федеральной службе безопасности Российской Федерации.

В процессе подготовки текста диссертации использованы методологические положения и выводы, содержащиеся в трудах отечественных и зарубежных ученых, политических и государственных деятелей, материалы научных дискуссий, конференций по информационной, проблематике, а также идеи, положения философской и политологической науки о политике как социальном явлении, связанные с информационной безопасностью.

Структура диссертации обусловлена предметом и общим замыслом темы, а также целью, задачами и внутренней логикой исследования проблемы. Она состоит из введения, трех глав, заключения и библиографического списка литературы. В первой главе исследуется взаимосвязь усиления роли информации в обществе и политики. При этом информационная безопасность рассматривается как общественное явление и обосновывается в качестве объекта политики. Отсюда обеспечение информационной безопасности вызывает к жизни политическую деятельность. В главе уточняется понятие "политика обеспечения информационной безопасности", дается его структура и содержание. Во второй главе, анализируя современные общественные условия, автор выявляет,

формулирует и раскрывает содержание наиболее общих императивов политики обеспечения информационной безопасности Российской Федерации. Кроме того, представлено обоснование и раскрыта структура механизма реализации императивов политики обеспечения информационной безопасности. В третьей главе представлено содержание приоритетных направлений политики обеспечения информационной безопасности России. Дается обоснование первостепенных мер реализации политики информационной безопасности Российской Федерации в современных условиях. В заключении приводятся обобщения, выводы, а также представлены теоретические и практические рекомендации и предложения, вытекающие из содержания диссертационного исследования.

2. НАУЧНАЯ НОВИЗНА ИССЛЕДОВАНИЯ И ОБОСНОВАНИЕ ПОЛОЖЕНИЙ, ВЫНОСИМЫХ НА ЗАЩИТУ

Научная новизна диссертационного исследования заключается в самой теме диссертации, которая в предложенной постановке рассматривается одной из первых в политологии, в совокупности разработанных автором лично теоретических основ политики обеспечения информационной безопасности, в выявлении ее императивов и приоритетов, а также полученных выводах и обоснованных практических предложениях, направленных на совершенствование политики обеспечения информационной безопасности Российской Федерации.

Более конкретно научная новизна состоит в:

а) результатах анализа научных представлений об информационной безопасности как явлении и объекте политики;

б) уточнении сущности и содержания понятия "политика обеспечения информационной безопасности";

в) выявлении, обосновании и формулировании наиболее общих императивов политики обеспечения информационной безопасности России;

г) раскрытии механизма реализации императивов отечественной политики обеспечения информационной безопасности;

д) определении приоритетных направлений современной российской политики обеспечения информационной безопасности;

е) обосновании первостепенных мер и практических предложений по формированию и реализации политики информационной безопасности Российской Федерации.

Обоснование положений, выносимых на защиту.

1. Обоснование информационной безопасности как объекта политики.

В современном обществе на передний план вышли малоизученные аспекты информации, такие как роль информации в детерминации

духовной, культурной, социально-политической, экономической жизни общества и обеспечении национальной безопасности. Именно поэтому, что затрагиваются самые чувствительные, существенные стороны общественной жизни, информационная безопасность является объектом и явлением политики. И это произошло не вдруг, не случайно. Характер движения социальных систем и его направленность всегда определяется циркулирующей в них информацией. Посредством информационного взаимодействия в обществе проявляется интеллект, осуществляются социализация личности, коммуникация, управление, познание и практическая деятельность. Каждый из этих процессов в качестве результата предполагает изменение самого объекта и его поведения.

Объяснение нового феномена информации в общественных отношениях автор осуществляет через ряд методологических подходов. Во-первых, психологический, сутью которого является то, что информация может оказывать воздействие на сознание людей, их мышление, волю и эмоции. Автор демонстрирует, что в ходе информационного взаимодействия идет процесс формирования личности, программирования внутренних структур психики, самосознания, внутреннего плана умственных действий, обуславливаемый усвоением структур и символов внешней социальной деятельности.

Второе объяснение коммуникативное. Оно тесно примыкает к первому, однако развивает и углубляет его. Суть в том, что на формирование интеллекта решающее влияние оказывает не просто коммуникация, а групповая коммуникация, в которой есть свои ролевые функции, нормы и правила, разделение целевых задач и др., которая осуществляется на основе и с помощью информации.

Третье объяснение социологическое. Люди живут по двум программам: биологической, направленной на приспособление к изменяющимся условиям жизни, и программе социальной, направленной не столько на приспособление, сколько на изменение условий своего бытия. Совместная жизнь в обществе, наследование культуры во всех ее проявлениях, развитая способность к творчеству, предсказанию, целеполаганию, конструированию, приобретают характер социальной программы, которую реализует человек в процессе своей жизнедеятельности. Однако и та, и другая программы реализуются в процессе информационных обменов.

Рассматривая информационную безопасность как общественное явление и объект политики, автор обосновывает важный вывод о том, что опасность деструктивного, разрушительного информационного воздействия на человека и общество существовала всегда. В принципе, можно утверждать, что проблема обеспечения информационной безопасности жизнедеятельности человека и общества является вечной. Этим

автор сознательно противопоставляет свою позицию тем исследователям, которые доказывают, что информационная безопасность есть проблема лишь современного информационно-технического мира.

Вместе с тем, в современном мире, под воздействием технического прогресса, проблема обеспечения информационной безопасности обострилась и действительно приобрела характер трудноразрешимой, в силу того, что затрагивает не только технические системы, но и все человеческие взаимодействия. Иными словами, проблема информационной безопасности имеет более глубинные основания, которые таятся в социальных отношениях, а раз так, то ее обеспечение неизбежно связано с политикой, не существует вне политики и без политики.

Полемизируя с авторами, предпринимающими усилия дать определение понятию информационная безопасность, автор обосновывает свое понимание этого явления как объекта политики. Это такое понимание информационной безопасности, которое имеет указание на состояние защищенности ее национальных интересов в информационной сфере, дополняет указанием на способность личности, общества и государства предотвращать ущерб жизненно важным информационным интересам, активно противостоять реальным информационным угрозам, проводить наступательную политику обеспечения своих интересов.

Диссертант обосновывает тезис о том, что информационная безопасность есть объект не только внутренней, но и международной политики.

Таким образом, в классически "чистом" виде проблема информационной безопасности стала осознаваться во второй половине XX века, вместе с формированием концепции "информационного общества", пришедшей на смену теориям "индустриального" и "постиндустриального" общества. Именно к этому периоду применение информационных технологий становится определяющим условием преобразования всех новейших наукоемких видов деятельности, а информация превратилась в решающий фактор социального развития, произошло осознание глубокой зависимости всех сфер жизнедеятельности общества от информации.

Политика обеспечения информационной безопасности становится обособленной, относительно самостоятельной сферой человеческой деятельности.

2. Авторское видение сущности и содержания понятия "политика обеспечения информационной безопасности".

Столкнувшись с реальными информационными опасностями, люди должны полагаться не на случай, а действовать разумно, сознательно, системно. Для этого необходима научно обоснованная политика обеспечения информационной безопасности. Политика, позволяющая реализовать принцип гуманизма для всех, улучшение социальной заботы

о членах общества, рост образования и здравоохранения, повышение благосостояния посредством увеличения производительности труда, облегчение всех форм общения, устранение языковых, культурных барьеров и др.

В силу того, что информационная безопасность есть явление многогранное и исторически изменяющееся, исследование политики ее обеспечения осуществляется на основе трех подходов: конкретно-исторический, теоретико-познавательный и социологический.

Первый аспект исследования политики обеспечения информационной безопасности связан с конкретно-историческими условиями возникновения и развития этого общественно-политического явления. Исследуя эволюцию деятельности по обеспечению информационной безопасности, диссертант обосновывает положение о том, что содержание и структура политики обеспечения информационной безопасности постепенно внутренне дифференцируется и качественно изменяется.

Другой аспект исследования содержания и структуры политики обеспечения информационной безопасности – теоретико-познавательный. Политика может целенаправленно воздействовать на объект и добиваться желаемого результата, только опираясь на достоверную информацию о самом объекте, путях и средствах его преобразования. Поэтому условием и существенным моментом содержания политики обеспечения информационной безопасности является познавательное отношение к социально-психологическим отношениям, явлениям и процессам, происходящим в обществе.

Для политики обеспечения информационной безопасности существенное значение имеет информация о социально-психологических процессах в обществе на двух основных уровнях общественного сознания: обыденного сознания и идейно-теоретического сознания.

Анализа третьего аспекта содержания и структуры политики обеспечения информационной безопасности – социологического, дает возможность преодолеть ограничения гносеологического анализа, полнее учитываются особенности этой политики. Он позволяет понять саму эту политику как специфический вид человеческой деятельности, как необходимый компонент творчества человека в рамках определенной социальной системы. Элементами этой системы являются люди в их связях и отношениях друг с другом по поводу вещей и идей. Политика обеспечения информационной безопасности направлена на защиту этих общественных связей и отношений, а также на создание условий для их успешного функционирования и развития. В основе социологического понимания содержания и структуры политики обеспечения информационной безопасности лежат интересы, прежде всего, личности и общества, а также государства.

Исходя из анализа трех подходов к политике информационной безопасности автор формулирует ее определение. Это деятельность социальных и институциональных субъектов по согласованию интересов личности, общества и государства и на этой основе использованию политической власти для предотвращения, нейтрализации и устранения последствий негативных информационных воздействий.

Главное содержание политики обеспечения информационной безопасности состоит в том, чтобы минимизировать опасности и угрозы, создать и поддерживать баланс информационных интересов личности, общества и государства.

Государство является важнейшим субъектом политики информационной безопасности. Ему принадлежит решающая роль в организации и проведении политики информационной безопасности. Для ее осуществления оно располагает необходимыми материальными ресурсами: людьми, средствами политико-правовой и технической защиты информации, образовательными учреждениями, финансами, средствами массовой информации и т.п.

3. Обоснование условий возникновения, формулирования и содержания императивов политики обеспечения информационной безопасности Российской Федерации.

В диссертации автор определяет императив политики обеспечения информационной безопасности как существующие явления, процессы, факторы, условия, которые выступают в качестве требований повелительного, безусловного и условного характера к деятельности по обеспечению информационной безопасности. Игнорирование императивов ведет к негативным последствиям для обеспечения информационной безопасности. Отсюда вытекает исключительная важность познания императивов политики обеспечения информационной безопасности России.

Приводя классификацию императивов политики обеспечения информационной безопасности, автор обосновывает необходимость раскрытия тех из них, которые имеют определяющее значение для Российской Федерации в современных условиях. К ним относятся: информационные, технологические, политические, а также потребности и интересы личности, общества и государства и опасности и угрозы им.

Информационные условия. Характеризуя их автор опирается на те факторы и признаки, которые раскрывают обстановку в мировом информационном пространстве. Прежде всего, речь идет о тех колоссальных изменениях в общественных отношениях развитых стран, которые происходят под воздействием информационной революции.

Определяя место и роль России в мировом информационном пространстве, следует подчеркнуть, что наша страна стремиться решительно присоединяется к мировым информационным тенденциям. Россия

в этом процессе стремиться занять достойное место, что требует осуществления информатизации общества более высокими темпами.

Характеризуя внутренние информационные условия в России, следует отметить, что проблема информатизации рассматривается политическим руководством как необходимое условие для устойчивого развития страны и ее вхождения в мировое информационное сообщество.

Информационная глобализация ведет к еще большему уплотнению "времени-пространства" с вытекающими отсюда противоречиями и проблемами для государств и обществ. Именно поэтому наблюдается противоположная тенденция – стремление сохранить свою национальную и региональную информационную самобытность. По сути это стремление социальных сил сохранить национальное государство как уникальный феномен индустриальной эпохи.

Анализируя противоречивость международных и внутриобщественных процессов автор полагает, что информационное развитие как объективный и закономерный процесс функционирования общества выступает базовым императивом политики обеспечения информационной безопасности России.

Технологические условия. Анализ технологических условий осуществляется на базе исследования фактов появления и влияния информационных технологий в развитых обществах и в нашем отечестве и используя методы сравнения и аналогий автор демонстрирует, что развитие техники и технологий стимулировали новые возможности использования информации. При этом технологические достижения оказались как позитивными, так и негативными.

Резюмируя анализ технологических условий общественного развития, диссертант приходит к выводу, что произошла технологизация управленческих, производственных, распределительных (обменных) и иных процессов в обществе и государствах. Обладание информационными технологиями, и особенно информационно-интеллектуальными технологиями, изначально обеспечивает преимущества в обеспечении информационной безопасности. Поэтому технологизация процесса информационного развития выступает императивом политики обеспечения информационной безопасности России.

Поскольку обеспечение информационной безопасности предполагает осуществление деятельности по согласованию интересов ее объектов, лежит в русле обеспечения безопасности более высокого уровня обобщения, то такую деятельность невозможно проводить вне властных отношений, а по существу вне политических отношений и процессов, образующих политические условия.

Характеризуя внешнеполитические условия, диссертант рассматривает процессы становления глобального информационного общества,

раскрывает информационное неравенство как результат возможностей и способностей одних стран производить, а других потреблять информационный продукт. Особое внимание уделяется информационным обменам и участию в них России. Главный вывод этих рассуждений состоит в том, что Россия с одной стороны стремиться встраиваться в формирующуюся информационную цивилизацию, а с другой выступает в большей степени потребителем информационных продуктов.

Внутриполитические условия характеризуются плюрализмом идеологий, взглядов, поиском новых места и роли государства в жизни российского общества. Характеризуя роль информации в основных сферах жизни российского общества, автор обосновывает, что она используется политическими силами для объединения своих сторонников в целях завоевания или удержания власти, реализации властеотношений, связанных с использованием имеющихся в их распоряжении материальных и финансовых ресурсов для формирования у различных социальных общностей и групп выгодных этим силам представлений, ценностей и предпочтений.

Общественные отношения, объектами которых являются информация и информационная инфраструктуры, сложившиеся в основных сферах общественной жизни и государственного управления, становятся предметом деятельности по обеспечению информационной безопасности.

Резюмируя изложенное, в диссертации делается вывод о том, что политическая обусловленность информатизации России выступает императивом политики обеспечения ее информационной безопасности.

В качестве важнейшего условия определяющего императивы политики обеспечения информационной безопасности России выступают информационные потребности и интересы личности, общества и государства.

Раскрывая эти условия, автор приходит к выводу, что информационные потребности и интересы оказываются зависимы от предмета своего удовлетворения – информации, а новая информация порождает потребность в еще более новой информации, что порождает постоянную динамику этих потребностей и интересов. В диссертации характеризуются основные национальные информационные потребности и интересы России, а также делается вывод об их изменении. Отсюда расширение спектра информационных потребностей и интересов личности, общества и государства выступает императивом политики обеспечения информационной безопасности Российской Федерации.

Наконец, условием возникновения императивов политики обеспечения информационной безопасности рассматриваются состояние опасностей и угроз информационным интересам России.

По сути информационные опасности и угрозы представляют собой всю совокупность негативного использования информации. При этом

объектами этого влияния могут выступать, как индивидуальное и массовое сознание, так и средства, системы хранения, обработки и передачи информации. Наиболее типичными информационными опасностями и угрозами принято считать:

- психотронное воздействие;
- дезинформирование;
- несанкционированный доступ к информации, сетям и системам;
- технико-технологические действия информационного характера.

Раскрытие содержания указанных опасностей и угроз дало возможность выдвинуть в качестве императива политики обеспечения информационной безопасности России расширение спектра и потенциала негативного использования информации.

В диссертации также обосновываются основные требования выявленных императивов политики обеспечения информационной безопасности России.

4. Результаты разработки механизма реализации императивов политики обеспечения информационной безопасности России.

Эффективное обеспечение информационной безопасности невозможно без комплексного использования политических, правовых, экономических, научно-технических, духовно-нравственных, информационных, военных и иных возможностей общества и государства или, иными словами, без соответствующего механизма или системы.

Анализируя подходы отечественных исследований, в частности В.Н. Веремьева, В.И. Голубева, Е.В. Макаренкова, В.Ф. Ницевича, В.С. Пуško, О.А. Рыжова, В.И. Солдаткина, В.Н. Ткачев, В.М. Шевцов и др., к сущности и содержанию понятия "механизм", автор, применительно к реализации императивов политики обеспечения информационной безопасности, исходит из того понимания, что это "совокупность таких компонентов, которые составляют наиболее важные параметры с точки зрения реализации повелительных требований"[1].

В структуре механизма реализации императивов политики обеспечения информационной безопасности в диссертации выделяются такие компоненты, как: мировоззренческо-ценностный; нормативно-правовой; институционально-организационный и функционально-деятельностный.

Мировоззренческо-ценностный компонент – представлен совокупностью мироощущения, мировосприятия и миропонимания. При этом, первые два элемента выражаются в эмоционально-психических параметрах, а третий опирается на знания.

---

[1] См.: Ницевич В.Ф. Императивы и приоритеты военно-информационной политики государства: Дисс. ... докт. полит. наук. – М.: ВУ, 2002. – С. 213-214.

Особость роли мировоззрения в рассматриваемом механизме определяется тем, что за последние десятилетия мир существенно трансформировался от индустриальной к информационной стадии развития. Эта трансформация не всегда своевременно и правильно осмысливается людьми, общностями и государствами и, как следствие, могут упускаться важнейшие объективные требования к смене норм общественной жизни.

Определяя отношение к действительности, как отдельного индивида, так и социальной общности, института мировоззрение выступает регулятором их практической деятельности. Такая деятельность не может быть в стороне от системы ценностей, обусловленной мироощущением, мировосприятием и миропониманием. С другой стороны, ценности во многом определяются теми традициями, обычаями, установками, которые присущи данному конкретному обществу. Реализация ценностно-ментальных основ в политике обеспечения информационной безопасности России находится на переходной стадии общественного развития. Поэтому в материализации идей, установок, в частности, в сфере информационной безопасности, осуществляется через систему ценностей.

Мировоззренческо-ценностный компонент механизма реализации императивов политики обеспечения информационной безопасности является тем звеном, которое обеспечивает познание, понимание и восприятие (принятие) информационных опасностей и угроз, а также формирование системы деятельности по упреждению, устранению или ликвидации негативных информационных проявлений в целях общественно значимых интересов.

Нормативно-правовой компонент представлен: нормами международного права, нормативными актами межгосударственного порядка; законодательными актами государственной власти; иными правовыми актами, которые регулируют текущие относящимися к сфере информационной безопасности; традициями и обычаями присущи российскому обществу, выполняющими регулятивную роль в информационной сфере.

Институционально-организационный компонент. Обеспечение информационной безопасности осуществляется специально созданными органами и институтами общества и государства. Однако ключевую роль в этом процессе играет государство, которое осуществляет управленческую и координационную деятельность. Поэтому основным институтом реализации императивов политики обеспечения информационной безопасности, организации и управления процессами в этой сфере следует считать государство. При этом следует учитывать, что в демократическом государстве, как правило, реализован принцип разделения властей, которые выполняют присущие им функции.

Вместе с тем, в развитых демократиях считается нормой широкое участие общественных институтов и органов в обеспечении информационной безопасности, например таких как: сам человек, гражданин, его объединения и институты. Поэтому в механизме реализации императивов политики обеспечения информационной безопасности большое значение придается деятельности негосударственных субъектов – общественных организаций и институтов. К ним относятся политические партии, общественные и общественно-политические движения, организации.

К основным организационным аспектам механизма реализации императивов политики обеспечения информационной безопасности относятся: разработка системного подхода к формированию и актуализации нормативно-правовой базы; информационное обеспечение органов и институтов, реализующих информационные установки и цели; регулирование информационной деятельности и стандартизации информационных процессов; контроль за выполнением решений в сфере информационной безопасности; подготовку специалистов в этой области деятельности, а также формирование потенциальных возможностей информационной деятельности государства и общества.

Функционально-деятельностный компонент рассматривается через призму выработки и выполнения решений в сфере политики информационной безопасности с использованием планирования, контроля, прогноза и корректировки функционирования всего механизма, которые содержательно раскрываются в диссертации.

Следует подчеркнуть, что механизм реализации императивов политики обеспечения информационной безопасности является достаточно сложным, а его функционирование находится под влиянием совокупности не только закономерных факторов, но и случайных, что предопределяет некоторую условность его рассмотрения в познавательных целях.

5. Обоснование структуры и содержания приоритетных направлений политики обеспечения информационной безопасности России.

Выявленные безусловные требования повелительного характера логично предопределяют основные приоритетные направления политики обеспечения информационной безопасности России. Такими приоритетными направлениями являются: информационное, технологическое, политическое, осмысление и реализация изменяющихся информационных интересов, предотвращения и нейтрализации информационных опасностей и угроз.

В раскрытии информационного направления уделяется внимание двум составляющим:

– защите информации, циркулирующей в обществе и, особенно, по сетям связи общего пользования;

– безопасности информационных обменов, при чем как внутри общества так с внешней средой.

Технологическое направление раскрывается через такие составляющие как: безопасность информационных технологий и информационного процесса, а также безопасность информационной техники и ее применения.

Политическое направление содержит в себе необходимость проявления политической воли и использования власти российского государства, обоснования и легитимности ограничений прав граждан на информацию, выработку законодательной базы и концептуальных основ политики информационной безопасности России.

Осмысление и реализация изменяющихся информационных интересов как направления политики обеспечения информационной безопасности России включает:

– мониторинг информационных потребностей личности, общества и государства;

– создание, совершенствование и модернизацию инфраструктуры информационного обеспечения государственного управления;

– организацию свободной и ответственной деятельности СМИ;

– информирование граждан и формирования общественного мнения;

– подготовку специалистов и формирования информационной культуры кадров государственной службы.

Предотвращение и нейтрализация информационных опасностей и угроз. В качестве исходного положения рассматриваемого направления является тот факт, что политика безопасности эффективна тогда, когда она создает возможности упредить возможные негативные и вредные воздействия. Отсюда в диссертации рассматривается необходимость упреждения опасных информационных состояний, которые могут возникнуть на разных этапах информационного процесса: поиска информации (наиболее частый вариант, когда человек не может получить необходимую информацию), ее хранения (информация либо источник информации имеется, но сохранить их не удается) или использования (информация находится в распоряжении человека, но он не может воспользоваться ею).

Кроме того, обосновывается противодействие таким основным угрозам безопасности в сфере информационных отношений, как: отказ от предоставления гражданам жизненно важной для них информации; предоставление искаженной информации; сокрытие информации.

Раскрытие приоритетов политики обеспечения информационной безопасности России позволило автору сделать важный вывод состоящий в том, что информационная безопасность должна обеспечивать

защиту как от прямого агрессивного информационного воздействия, так и от неконтролируемой утечки информации, некомпетентности держателя информации относительно ее действительного содержания и возможностей воздействия на тот или иной объект. Меры информационной защиты должны улавливать разные варианты субъективного отношения воздействующего субъекта к своим действиям по хранению и распространению информации, последствиям этих действий.

6. Основные положения разработанных автором первоочередных мер политики обеспечения информационной безопасности России в современных условиях.

Реализация приоритетных направлений политики обеспечения информационной безопасности России необходимо требует пересмотра сложившихся концептуальных основ государственной политики, разработки новых механизмов в отношении регулирования рынка информационных технологий, информационной и инвестиционной политики, развития информационного законодательства и обеспечения защиты информации. В диссертации первоочередные меры объединены в ключевые и обеспечивающие группы. К ключевым относятся:

– создание условий для роста безопасности информационной инфраструктуры и индустрии;

– улучшение безопасности доступа к информационной инфраструктуре и сетевым услугам;

– создание условий для безопасности развития и использования возможностей, предоставляемых информационным обществом;

– поддержка безопасности научных исследований и социально-значимых приложений информационных технологий;

– развитие информационно-телекоммуникационных систем и обеспечение безопасности информационных ресурсов в интересах государственного управления.

В качестве обеспечивающих первоочередных мер автор обосновывает:

– совершенствование законодательства и регулирования в сфере безопасности информации и информатизации;

– обеспечение защиты информации;

– расширение международного сотрудничества в области информационной безопасности;

– создание эффективной организационно-институциональной системы обеспечения информационной безопасности России.

Таким образом, в обеспечении информационной безопасности России особое значение имеют те первостепенные меры политики, которые создают условия для реализации современных ее императивов.

3. ПРАКТИЧЕСКАЯ ЗНАЧИМОСТЬ ИССЛЕДОВАНИЯ И ЕГО АПРОБАЦИЯ

Научно-практическая значимость определяется тем, что в отечественной науке это одна из первых работ, посвященных исследованию императивов и приоритетов политики обеспечения информационной безопасности России.

Теоретические выводы и практические рекомендации, вытекают из целостного видения политики обеспечения информационной безопасности, в которой существенное значение приобретают объективные и субъективные детерминанты, предопределяющие ее приоритеты. Результаты исследования могут быть использованы для совершенствования Доктрины информационной безопасности Российской Федерации, а также для формирования и эффективной реализации политики обеспечения информационной безопасности в современных условиях.

Кроме того, результаты исследования могут найти применение в преподавании политологии, философии, социологии, других гуманитарных и социальных наук в высших военно-учебных заведениях Российской Федерации; в системе подготовки, повышения квалификации и переподготовки государственных служащих, а также в научно-исследовательской деятельности, для активизации усилий по дальнейшей теоретической разработке проблемы.

Апробация результатов исследования. Основные положения и выводы, полученные на различных стадиях диссертационного исследования, обсуждались на кафедре социальных наук и государственного управления Московского государственного областного университета, апробированы на конференции в Орловском государственном техническом университете. Основные положения и выводы изложены в публикациях:

1. Судоргин О.А. Некоторые приоритетные направления обеспечения информационной безопасности России. // Материалы международной научно-теоретической конференции "Национальная идея в контексте модернизации российского общества" /Под ред. О.В. Фирсановой. – Орел: ОрелГТУ, 2005. – С. 275 – 281. – 0,37 п.л.

2. Судоргин О.А. Развитие концепции обоснованного риска как обстоятельства, исключающего преступность деяния, в российском уголовном законодательстве. //Материалы 11 международной научно-практической конференции. – М.: МГУ, 2002. – С. 256 – 260. – 0,25 п. л.

3. Судоргин О.А. Политика обеспечения информационной безопасности: понятие, императивы, приоритеты. /Научное издание. – Орел: ОРАГС, 2005. – 88 с. – 5,5 п.л.