На правах рукописи

ПРОЦЕНКО ЕВГЕНИЙ ВАСИЛЬЕВИЧ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПОЛИТИЧЕСКОЙ КОММУНИКАЦИИ В СОВРЕМЕННОЙ РОССИИ

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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата политических наук

Ставрополь - 2009

Диссертация выполнена на кафедре философии ГОУ ВПО «Невинномысский государственный гуманитарно-технический институт»

Научный руководитель	доктор политических наук, профессор **Чагилов Валерий Расулович**
Официальные оппоненты:	доктор философских наук, профессор **Стризое Александр Леонидович**
	кандидат политических наук **Бабкин Игорь Олегович**
Ведущая организация:	**Филиал ФГОУ ВПО «Северо-Кавказская академия государственной службы» в г. Пятигорске**

Защита диссертации состоится 9 сентября 2009 года в 14 00 часов на заседании совета по защите докторских и кандидатских диссертаций Д 212 256 06 при Ставропольском государственном университете по адресу 355009, г Ставрополь, ул Пушкина, 1, корп 1-а, ауд 416

С диссертацией можно ознакомиться в научной библиотеке Ставропольского государственного университета

Автореферат разослан 7 августа 2009 г

Ученый секретарь
совета по защите докторских и
кандидатских диссертаций Г Д Грищенко

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность исследования. В процессе информационной глобализации в мире фактически возникло единое информационное пространство, которое привело к унификации информационных и телекоммуникационных технологий всех стран – субъектов информационного общества

Появление общемирового информационного пространства с неизбежностью повлекло видоизменение элементов политической системы В частности, наряду с появлением новых политических акторов и трансформацией традиционных политических институтов возникли новые формы политической борьбы, механизмы и способы политического влияния В результате в структуре политической системы обозначились тенденции масштабного усложнения ряда ее подсистем и, прежде всего, политической коммуникации

Существенные изменения политико-коммуникативной подсистемы политической системы современной России, расширение числа акторов политического процесса за счет вовлечения в ее состав все большего количества новых участников, с одной стороны, и появление объективных вызовов и угроз безопасности российского государства, с другой – в значительной степени предопределило приоритет проблемы обеспечения информационной безопасности политической коммуникации в качестве не только задачи политической практики, но и актуальной научной проблемы

Глобализация информационного пространства дала возможность ведущим державам (прежде всего, Соединенным Штатам Америки, Японии и Китаю) наращивать свое военное, политическое, экономическое и научно-технологическое превосходство посредством лидерства в области информационно-телекоммуникационных технологий и навязывать свои ценности, осуществляя глобальный информационный контроль над мировым сообществом

Высокая эффективность средств информационного воздействия, широкий спектр их применения и скрытость оказываемого влияния являются причинами пристального интереса ученых многих стран к исследованиям в области разработки теории и практики применения информационного оружия и, как следствие, теории ведения информационных войн

Возрастание в этих условиях теоретической актуальности и практико-политической значимости проблематики обеспечения национальной безопасно-

сти в целом, и в частности информационной безопасности политической коммуникации России, обусловило выбор темы диссертационного исследования

Степень научной разработанности проблемы. Одним из приоритетных направлений современного политологического знания является исследование феномена политической коммуникации и обеспечения ее информационной безопасности

Рассмотрение политической коммуникации в качестве способа достижения согласия между индивидами, а также управляющими и управляемыми посвящены работы Р -Ж Шварценберга, в качестве способа развертывания логической последовательности политических событий в трудах Н В Анохина, О А Маканова Понимание политической коммуникации как всего диапазона неформальных коммуникативных процессов в обществе присутствует в трудах Л Пая, а как часть массовой коммуникации в работах П Лазерсфельда

Среди отечественных исследователей понятие «политические коммуникации», а также их функционирование анализируется в работах М Эпштейна, обращающегося к проблеме избыточности информации, М Вершинина, изучающего политические коммуникации, в том числе и в информационном обществе В Латынов, А Соловьев, М Хончаров, в своих исследованиях обращаются к анализу политической коммуникации как сфере обращения информации

Отечественная и зарубежная наука уделяет большое внимание постиндустриальному развитию информационной безопасности как проблеме становления информационного общества Различным аспектам информационного общества как нового типа социальной организации посвящены работы зарубежных ученых Л Боек, М Вебера, Н Винера, У Мартина, И Мсуды, Н Мура, Д Полаг, Д Робертсона, Г Саймона, Т Стоуньера, А Тоффлера, Ю Хабермаса, С Хилгартнера, отечественных ученых Р Ф Абдеева, Г Г Васильева, Т П Ворониной, С Н Гриняева, О В Кедровского, К К Колина, А А Левина, И С Мелюхина, Н Н Моисеева, Ю А Нисневича, В Д Попова, А И Ракитова, Г Л Смоляна, Д С Черешкина, Е В Халиповой, Р Хонтель, А С Шийко и др

За последнее время серьезному изучению подвергнуты проблемы правового обеспечения государственной информационной политики и развития информационного законодательства, интенсивно разрабатываются теоретические ос-

новы, методологические и практические рекомендации, касающиеся вопросов информационного взаимодействия государственной власти и гражданского общества, институциональных структур гражданского общества, средств массовой информации и коммуникации Различные аспекты этих проблем нашли отражение в трудах М Г Анохина, С Блэка, Г Вильсона, В М Горохова, Дж Грюнига, М Г Зяблюка, Р Келли, В С Комаровского, В А Кулинченко, Э Ноэль-Нольмана, А С Пую, Н Стоуна, Т Ханта, Д Хелда и других исследователей

Научно-методологические основы информационного обеспечения и совершенствования информационной безопасности на основе внедрения современных ИКТ деятельности системы органов государственной власти, информатизации государственного управления, включая региональные аспекты этой проблемы, защиты информации и международного информационного обмена, развития информационно-коммуникационной инфраструктуры, системы информационных ресурсов, сетей связи и телекоммуникаций как единых общегосударственных систем подробно исследованы в трудах И А Андреевой, А Б Антопольского, Г Т Артамонова, И Р Ашурбейли, Г В Белова, Л А Василенко, А В Возженикова, Г С Галиуллиной, В В Гудкова, А Р Даниелова, И И Егорова, В Д Ильина, М Я Клепцова, В Н Костюка, Б В Кристального, А П Курило, И Н Курносова, В Д Попова, А Л Райкова, А К Скуратова, Л И Шехтмана, А С Шийко и других

Научное осмысление проблемы информационной безопасности как явления политической жизни общества значительно активизировалось в последнее десятилетие, в отличие от исследований, проводимых в сфере технических наук В течение последних 5 лет отечественными учеными А В Возженниковым, Ю Ф Нуждиным,,, И Н Панариным, А И Поздняковым, Г Г Почепцовым, А А Прохожевым, С П Расторгуевым, Г Л Смолян, А А Стрельцовым, Д С Черешкиным, В Н Цыгичко и другими весьма активно и результативно проводились политологические исследования, касающиеся информационной безопасности

Рассмотрению проблем защиты личности от негативного информационного воздействия в современном мире посвящены работы Г В Грачева, Ю А Ермакова, В Е Ленского, И К Мельника, И Н Панарина, А С Панарина и других исследователей

Правовым аспектам защиты интересов личности в информационной сфере общества посвящены работы В А Анниковой, А А Антопольского, А Л Балыбердина, И Л Бачило, М С Григорьева, В И Кирина, О А Колобо-

ва, В А Копылова, В Н Лопатина, Д В Огородова, А В Попова, Ю Г Просвирина, А А Фатьянова, В Н Ясенева В большей степени их усилия были сосредоточены на правовом обеспечении защиты сведений, совершенствовании законодательства в области информатизации

Проблемам борьбы с информационными преступлениями в современном обществе посвящены исследования В М Боер, В В Борискина, Л Л Ефимовой, В П Иванского, Ю В Калининой, Л Р Клебанова, С Н Кленова, М Ю Костенко, С В Кузьмина, П У Кузнецова, А А Левина, О В Ревинский, Т Н Ревяко, М К Рожковой, А А Тераkопова, Б Х Толбековой, С И Ушакова, А С Шийко

Техническим аспектам защиты информации в информационных системах и сетях посвящены работы В А Герасименко, С Н Гриняева, В Л Лопатина, В А Никитова, Е Л Орлова, Г Л Савина, А В Старовойтова, М Л Сычева, Л М Ухлинова, Ю Л Шершневой, Н Г Шурухнова, В Д Цыганкова, В Л Цыгичко

Вместе с тем проблема информационной безопасности системы политической коммуникации до сих пор остается в отечественной политической науке малоизученной и требует своего дальнейшего комплексного исследования

Таким образом, актуальность, степень научной разработанности и значение проблемы определили содержание исследования, его структуру, объект, предмет, цель и задачи работы

Объектом исследования выступает политическая коммуникация в условиях современного российского общества

Предметом исследования является содержание государственной политики по оптимизации механизмов информационной безопасности политической коммуникации в современной России

Цель исследования состоит в выявлении основных направлений и способов оптимизации политики государства по обеспечению информационной безопасности политической коммуникации в современной России

Для достижения данной цели необходимо решение следующих **задач**

- в контексте современных глобальных информационных процессов уточнить содержание понятия «информационная безопасность политической коммуникации»,
- проанализировать основные угрозы информационной безопасности политической коммуникации в современной России,

- рассмотреть роль информационного компонента политической коммуникации в условиях социально-политической трансформации российского общества,
- выявить основные способы обеспечения информационной безопасности политической коммуникации российского общества,
- рассмотреть основные направления деятельности государства по оптимизации информационной безопасности политической коммуникации современной России,
- уточнить содержание возможной концептуальной модели региональной системы информационной безопасности политической коммуникации на Северном Кавказе

Теоретико-методологическую основу исследования составили теории политической системы Т Парсонса, информационно-кибернетической природы политической системы К Дойча, коммуникативных процессов в политической системе Н Лумана, Ю Хабермаса и др Использование указанных теоретических моделей позволило осуществить содержательный анализ информационно-коммуникативных компонентов и процессов политической системы общества и определить место и роль информационной безопасности политической коммуникации в ее сохранении и функционировании

Существенную роль в реализации исследовательских задач диссертационного исследования сыграло применение системного подхода, использование которого дало возможность достичь более полного представления о «политической коммуникации», «информационной безопасности», «информационном обществе», «информационной войне» В представленной работе используются труды ведущих отечественных исследователей при уточнении понятий «информационная безопасность» (Г В Емельянов, И Н Панарин, А А Стрельцов, Ю А Фисун, и т д), «информационная война» (Н А Брусницина, И Н Панарина, А И Петренко, А А Стрельцов, А В Манойло,)

Широкое применение в работе исторического, бихевиористского, синергетического и компаративистского подходов обеспечило возможность исследовать тему диссертационного исследования в качестве целостного исторического и самоорганизующегося феномена, предназначенного обеспечить информационную безопасность политической коммуникации современной России

Нормативно-правовую базу исследования оставили

Указ Президента РФ от 12 мая 2009 г , № 537 «Стратегия национальной безопасности Российской Федерации до 2020 года», Доктрина информационной безопасности РФ (1996, 2000, 2009 гг), Федеральный закон от 27 июля 2006 г N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральная целевая программа «Электронная Россия (2002-2010 годы)», Федеральный закон Российской Федерации от 27 июля 2006 г N 152-ФЗ «О персональных данных», Закон Российской Федерации «О государственной тайне» от 21 июня 1993 г № 5485-I (с изменениями и дополнениями от 6 октября 1997 г № 131-ФЗ, от 30 июня 2003 г № 86-ФЗ, от 11 ноября 2003 г № 153-ФЗ, от 29 июня 2004 г № 58-ФЗ, от 22 августа 2004 г № 122-ФЗ), Федеральный закон N 164-ФЗ от 1 октября 2008 «О ратификации Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации», Указ Президента РФ № 351 от 17 марта 2008 года «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», Постановление Правительства РФ № 781 от 17 ноября 2007 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

Научная новизна исследования заключается в следующем

- уточнено содержание понятия «информационная безопасность политической коммуникации» как состояния защищенности системы государственных и политических институтов общества от информационных внутренних и внешних угроз,
- систематизированы угрозы информационной безопасности политической коммуникации в современной России и установлено их обусловленность одновременной активизацией и обострением информационного противоборства,
- доказано, что информационный компонент политической коммуникации приобретает приоритетный характер в условиях социально-политической трансформации российского общества,
- установлено, что одним из эффективнейших способов обеспечения информационной безопасности политической коммуникации является механизм информационного «щита» и «фильтра»,

- обоснованы возможные направления оптимизации государственной политики в сфере информационной безопасности политической коммуникации современной России,
- уточнены компоненты концептуальной модели региональной системы информационной безопасности политической коммуникации на Северном Кавказе

Основные положения, выносимые на защиту:

1 Постиндустриальное развитие современной цивилизации кардинально трансформировало значимость информационной сферы общества и обусловило ее переход из технико-вспомогательной в разряд приоритетных с точки зрения политического управления В условиях усиливающегося не только глобального информационного взаимообмена, но и противоборства современных государств информационная безопасность политической коммуникации как состояние защищенности интересов государства и общества в информационной сфере от внутренних и внешних угроз выступает в качестве основного компонента системы безопасности государственных и политических институтов общества, а в широком контексте системы национальной безопасности страны

2 Угрозами информационной безопасности политической коммуникации современного российского общества являются активизация источников и обострение разнообразных новейших способов информационного противоборства, основывающегося на современных видах информационного оружия Как система угрозы информационной безопасности политической коммуникации представляет собой взаимосвязанный комплекс внешних и внутренних источников угроз, а также совокупность информационных, программно-математических, физических, радиоэлектронных и организационно-правовых способов воздействия на объекты политической коммуникации

3 В контексте социально-политической трансформации российского общества информационный компонент политической коммуникации объективно становится чрезвычайно значимым элементом взаимодействия общества и власти, поскольку в этих условиях государство испытывает острую потребность в широком и эффективном информационном обеспечении целей и задач транзита Широкая социально-политическая востребованость в период трансформации информационной сферы как совокупности информационных потребно-

стей и интересов становится фактором неизбежного появления нового вида национальной безопасности - информационной безопасности

4 Наряду с организационно-политическими и нормативно-правовыми способами обеспечения информационной безопасности, не менее важным выступает технологический механизм защиты систем государственного управления, институтов и структур политической власти от несанкционированного воздействия с целью причинения негативного информационного ущерба Таковым механизмом защиты политической коммуникации являются информационный «щит» и «фильтр» Под «фильтром» понимаются маршрутизаторы и специальные программы, которые блокируют свободный поток информации, а под информационным «щитом» - брандмауэр – виртуальное подобие «великой стены», предназначенный для постоянной цензуры и полного контроля над информационными потоками

5 В условиях социально-экономических и общественно-политических преобразований в России определяющая роль в формировании и реализации политики информационной безопасности принадлежит органам государственной власти, выступающим одновременно в качестве ее субъекта и объекта К важнейшим направлениям оптимизации государственной политики в сфере информационной безопасности политической коммуникации следует отнести эффективное прогнозирование состояния современных информационных угроз, в частности, касающихся, информационного терроризма, развитие доктринальных основ информационной безопасности в общей системе безопасности современной России, развитие и систематическое совершенствование правовых основ обеспечения информационной безопасности

6 Региональная информационная безопасность политической коммуникации, выступает частью системы обеспечения национальной безопасности, ее подсистемой, безопасность которой обеспечивается в соответствии с российским законодательством и учетом федеративной формы политико-территориальной организации государства По своему построению региональная система информационной безопасности политической коммуникации является многоуровневой и многофункциональной системой Структура региональной системы включает территориальные органы управления, решающие общесистемные задачи региональной системы информационной безопасности

Теоретическая значимость исследования определяется возможностью расширения теоретического представления о политической коммуникации и

проблемах, связанных с обеспечением ее информационной безопасности, а также совершенствования понятийного аппарата и методологии Полученные в работе результаты, сформулированные выводы могут способствовать развитию необходимых теоретических и методологических основ для определения путей совершенствованию политики в области информационной безопасности политической коммуникации Основные положения и выводы могут быть использованы в дальнейшем исследовании проблемы глобального информационного пространства

Практическая значимость исследования состоит в том, что основные результаты диссертационного исследования могут использоваться в процессе формирования и совершенствования концепции национальной безопасности, разработки программы развития российского информационного законодательства, а также в практической деятельности органов государственной власти и институтов гражданского общества по выработке и реализации мер противодействия, адекватных современным информационным угрозам Материалы диссертации могут стать основой для разработки учебных курсов и спецкурсов по политологии и политической социологии в вузах и структурах послевузовского профессионального образования

Апробация исследования. Диссертация обсуждена на заседании кафедры философии ГОУ ВПО «Невинномысский государственный гуманитарно-технический институт» и рекомендована к защите по специальности 23 00 02 – Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии

Основные положения диссертации были представлены в тезисах и статьях в пяти конференциях и семинарах, в том числе V городской научно-практической конференции «Студенческая наука – экономике города Невинномысска» (г Невинномысск, 2006 г), региональной студенческой конференции «Проблемы современного общества глазами молодежи» (г Ставрополь, 2006 г), региональной научно-практической конференции «Социальная эволюция, идентичность и коммуникация в XXI веке» (г Ставрополь, 2007 г), международной научно-практической конференции «Проблемы обеспечения национальной безопасности, гражданского мира и согласия в контексте глобализационных вызовов и угроз постсовременности» (г Невинномысск, 2007 г), международной научно-практической конференции «Молодежь и наука реальность и будущее» (г Невинномысск, 2008 г)

Основные результаты исследования отражены в шести научных публикациях общим объемом 4,5 п л , в том числе в одной статье, опубликованной в ведущем рецензируемом научном журнале, определенном Высшей аттестационной комиссией

Объем и структура работы. Диссертация состоит из двух глав, шести параграфов, заключения, библиографического списка использованной литературы, включающего 221 наименование, в том числе 10 - на иностранном языке Общий объем работы составляет 199 страниц машинописного текста

II. ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во «**Введении**» обоснована актуальность темы исследования, определена степень разработанности проблемы, сформулированы цель и задачи исследования, его новизна, обозначена теоретико-методологическая основа диссертации, сформулированы положения, выносимые на защиту, выявлена теоретическая и практическая значимость работы, описана ее апробация, раскрыта структура работы

Первая глава «Теоретико-методологические основы исследования информационной безопасности политической коммуникации в современной России» содержит три параграфа, которые посвящены уточнению понятийного аппарата исследования, рассмотрению условий и причин возникновения феномена «информационной безопасности политических коммуникаций», а также освещают влияние процессов информатизации и глобализации на политические коммуникации современной России

В первом параграфе «Сущность информационной безопасности и методология ее анализа в системе политологического знания» описаны теоретические подходы к объяснению сущности исследования информационной безопасности в России и в современном мире

Информационная безопасность как самостоятельная область научного познания базируется на общей теории безопасности А Крутских, А А Прохожева, кибернетики А И Позднякова и информатики С В Смульского В условиях становления глобального информационного общества информационная безопасность выступает важнейшей потребностью и жизненно важным интересом личности, общества и государства Она, согласно А Федорова и В П Шерстюка, представляет собой теоретические положения и методологические основы, обеспечивающие процесс изучения, исследования,

анализа, разработки предложений, рекомендаций и концепций защиты интересов субъектов информационно-коммуникационных процессов

Так, под «информационной безопасностью» В Л Манилов и А А Стрельцов понимают систему информационных потоков печатных, электронных и иных средств массовой информации, обеспечивающих стабильное состояние жизнедеятельности личности, общества и государства во всех сферах

Согласно утверждению В Н Лопатина, впервые исследовавшего правовые проблемы формирования основ информационной безопасности России и ее законодательного обеспечения, в органах государственной власти сложились два *определения понятия информационной безопасности* Первое связывает вопросы информационной безопасности только с защитой информации, причем не всей, а лишь той, которая составляет государственную и военную тайну, а второе - рассматривает информационную безопасность как «состояние защищенности информационной среды, соответствующей интересам государства независимо от воздействия внутренних и внешних информационных угроз»

По мнению известного отечественного теоретика и практика И Н Панарина, в условиях информационного противоборства в политической и военной сферах «информационная безопасность» – это состояние защищенности информационной среды общества и политической элиты, обеспечивающее ее формирование и развитие в интересах политической элиты, граждан и государства

В исследованиях ряда авторов (М А Вус, В С Гусев, Д В Долгирев, А А Молдовян и др) под информационной безопасностью в узком смысле нередко понимается набор аппаратных и программных средств обеспечения сохранности, доступности и конфиденциальности данных в компьютерных сетях По их мнению, то, что в 1970-е годы называлось компьютерной безопасностью, а в 1980-е – безопасностью данных, сейчас именуется информационной безопасностью Информационной безопасностью М А Вус и др называют «меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе»

Например, В А Галатенко и В К Левин под информационной безопасностью понимают «защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры», выделяя тем самым уже два объекта защиты – информацию и информационную инфраструктуру

В контексте предложенной В Л Маниловым, А А Стрельцовым интерпретации понятия «информационная безопасность» под информационной безопасностью политической коммуникации политической системы понимается способность институтов политической власти защитить, совокупность процессов информационного обмена, передачи политической информации, структурирующих политическую деятельность, реализовать конституционные права и свободы человека и гражданина в области получения и использования информации в целях своего гармоничного развития Одновременно информационная безопасность политической коммуникации направлена на сохранение незыблемости конституционного строя, суверенитета и территориальной целостности страны, политической, экономической и социальной стабильности, законности и правопорядка, развития равноправного и взаимовыгодного международного сотрудничества

Некоторые ученые, в частности, Д А Ловцов, считают, что состояние информационной безопасности личности, общества и государства, определяется, главным образом, двумя факторами информационно-психологической удовлетворенностью потребностей граждан и негативными (преднамеренными и случайными) информационно-психологическими и информационно-техническими воздействиями В связи с этим под информационной безопасностью, в «широком» смысле слова, Д А Ловцов и др ученые понимают защищенность потребностей граждан, отдельных групп и социальных слоев, массовых объединений людей и населения в целом в качественной (ценной) информации, необходимой для их жизнедеятельности (функционирования), образования и развития, то есть, определяя информационную безопасность через потребности, в данном случае забыты интересы государства как самостоятельного объекта защиты

На основе теоретического анализа подходов к определению понятия «информационная безопасность» в работе предлагается уточненная дефиниция понятия «информационная безопасность политической коммуникации», под которой понимается состояние защищенности интересов государственных и политических институтов общества в информационной сфере от внутренних и внешних угроз

Во втором параграфе «Угрозы информационной безопасности политической коммуникации в современной России» показано, что формирование информационного общества создает новую проблему для науки - про-

блему разработки своевременных методов, технологий и процедур исследования информационной безопасности как составной части национальной безопасности в целом

Информация с ее техническими атрибутами как бы «вживается» в ткань общественных отношений Информационные ресурсы, информационные и коммуникационные технологии вошли в структуру большинства рычагов влияния, в том числе экономических, сами стали объектами всемирного рынка, позволяющим воздействовать на механизмы политического управления во всех его видах и сферах

Активизация источников и обострение разнообразных новейших способов информационного противоборства и, как его крайней формы, информационной войны, основывающихся на современных видах информационного оружия, в работе рассматриваются в качестве угроз информационной безопасности политической коммуникации современного российского общества

Информационное оружие - это средства уничтожения, хищения или искажения информации, воспрещения или ограничения доступа к ней законных пользователей, разрушения информационных систем или дезорганизации работы связанных с ними средств высокотехнологичного функционирования государства и жизнеобеспечения общества, воздействия на сознание и подсознание людей в интересах противника Это оружие - определяющий фактор не только межцивилизационной конкуренции, но зачастую фактор, предрешающий исход и самих военных кампаний в классическом понимании данного явления Всевозможные манипуляции информационным оружием в условиях информационного общества – это прием, который все чаще и чаще используется государствами в мирное время

Под системой угроз информационной безопасности политической коммуникации понимается целостный комплекс внешних и внутренних источников угроз, а также информационные, программно-математические, физические, радиоэлектронные и организационно-правовые способы воздействия на объекты политической коммуникации

Источники угроз информационной безопасности политической коммуникации в современной России можно разделить на внешние и внутренние

К наиболее значимым внешним источникам относятся недружественная политика иностранных государств в области глобального распространения информации и новых информационных технологий, деятельность иностранных

разведывательных и специальных служб, деятельность иностранных политических структур, направленная против интересов Российского государства, преступные действия международных групп, формирований и отдельных лиц, стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков, деятельность международных террористических организаций, разработка рядом государств стратегий ведения информационных войн и создание технических средств и способов негативного воздействия на институты и структуры публичной власти страны

К важнейшим внутренним источникам относятся критическое состояние отечественных отраслей промышленности, неблагоприятная криминогенная обстановка, сопровождающаяся усилением влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере, недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации, недостаточная разработанность нормативно-правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика, неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России, снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности, недостаточная активность федеральных органов государственной власти в формировании открытых государственных информационных ресурсов и развитии системы доступа к ним граждан, отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления

Способы воздействия угроз на объекты информационной безопасности политической коммуникации в Российской Федерации подразделяются на информационные, программно-математические, физические, радиоэлектронные, организационно-правовые

К информационным способам относятся нарушения адресности и своевременности информационного обмена, противозаконный сбор и использование информации, несанкционированный доступ к информационным ресурсам, манипулирование информацией (дезинформация, сокрытие или искажение информации), незаконное копирование данных в информационных системах, использование средств массовой информации с позиций, противоречащих интересам граждан, организаций и государства

Программно-математические способы включают внедрение программ-вирусов, установку программных и аппаратных закладных устройств, уничтожение или модификацию данных в информационных системах,

Физические способы включают уничтожение или разрушение средств обработки связи, хищение программных или аппаратных ключей и средств криптографической защиты информации, воздействие на персонал, поставка «зараженных» компонентов информационных систем

Радиоэлектронными способами перехват информации в технических каналах ее утечки, внедрение электронных устройств перехвата информации в технических средах и помещениях, перехват, дешифрование и навязывание ложной информации в сетях передачи данных и линиях связи, воздействие на парольно-ключевые системы, радиоэлектронное подавление линий связи и систем управления

Организационно-правовые способы закупки несовершенных или устаревших информационных технологий и средств информатизации, невыполнение требований законодательства и задержки в принятии необходимых нормативно-правовых положений в информационной сфере, неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию

В работе доказано, что системная и целенаправленная реализация указанных угроз может привести к дезорганизации системы государственного управления, к подрыву государственного авторитета Российской Федерации на международной арене, провоцированию социальных, этнополитических, религиозных и иных конфликтов в обществе

В третьем параграфе «Информационный компонент политической коммуникации в условиях социально-политической трансформации» рассматривается информационный компонент политической коммуникации в условиях социально-политической трансформации России

В контексте социальной трансформации информационный компонент рассматривается в качестве значимого элемента политической коммуникации

Концепция П Вацлавика рассматривает коммуникацию как контекст любых социальных процессов В таком понимании коммуникация рассматривается в двух аспектах как фон социального взаимодействия и процесс взаимодействия, интеракция Недостаточность такого анализа коммуникации проявляется в узко-психологическом понимании коммуникации, когда она отождествляется с процессом общения Одновременно с этим разрабатываются иные модели коммуникации концепция Н Лумана и Ю Хабермаса В рамках этих концепций, коммуникация осмысляется как механизм социального взаимодействия, основа современных форм социальности и описываются возможные способы решения социальных проблем современного общества, в частности, проблемы коммуникации в информационном обществе

Активно внедряясь в сферу политики, новые информационно-коммуникационные технологии не только качественно видоизменили старые представления, установки, стереотипы, но и сломали многие формы поведения, модели взаимоотношений между политическими институтами и индивидами По мнению А А Чеснакова, начинается формирование нового обширного канала политической коммуникации, динамика развития которого может перевернуть представления как о системе обеспечения политической деятельности, так и о традиционных инструментах политического участия В широком смысле, как подчеркивал известный американский политолог Л Пай, политическая коммуникация подразумевает не одностороннюю направленность сигналов от элит к массе, а весь диапазон неформальных коммуникационных процессов в обществе, которые оказывают самое разное влияние на политику Иными словами, совокупность процессов информационного обмена, передачи политической информации, структурирующих политическую деятельность и придающих ей смысловое значение, как передача смыслов, значимых для функционирования политической системы

В узком значение политическая коммуникация может быть рассмотрена как информационная инфраструктура политической системы, включающая центры обработки и анализа информации, каналы информационного обмена и телекоммуникации, механизмы обеспечения функционирования телекоммуникационных систем и сетей, в том числе системы и средства защиты информации

Под информационным компонентом политической коммуникации в новых нормативно-правовых документах РФ (Доктрина информационной безопасности РФ (1996, 2000, 2009 гг), концепция информационной безопасности РФ (Проект 21 12 95)) понимается система информационных ресурсов вне зависимости от форм хранения, содержания информации, составляющие государственную тайну и ограниченного доступа, коммерческую тайну и другую конфиденциальную информацию, а также открытую (общедоступную) информацию и знания

Период социальной трансформации представляет собой совокупность таких реформаторских преобразований, которые детерминируют характер, направленность протекания и конечные параметры экономических, социальных, политических и духовно-идеологических процессов того или иного общества При этом период социально-политического транзита выступает аналогом цивилизационного этапа, периода возникновения нового социально-экономического строя, нового политического режима, качественно новой социальной структуры, новейшей социокультурной и ценностной среды

В период масштабных социальных преобразований чрезвычайно значимым элементом взаимодействия общества и власти объективно становится, информационный компонент политической коммуникации, поскольку в этих условиях государство испытывает острую потребность в широком и эффективном информационном обеспечении целей и задач транзита Иными словами, информация выступает важнейшим фактором оптимизации государственного управления трансформационными процессами, так как позволяет органам государственной власти средствами и методами информационной политики оптимизировать, во-первых, целенаправленное управление информационной средой, которая включает в себя формирование и распространение различных видов информационных воздействий, а, во-вторых, управление информационными потоками и ресурсами, обеспечивающими развитие информационно-коммуникационной подсистемы политической системы общества в условиях транзита

Широкая социально-политическая востребованость в период трансформации информационной сферы как совокупности информационных потребностей и интересов становится фактором неизбежного появления нового вида национальной безопасности - информационной безопасности

Информационная безопасность современной России в целом, и информационная безопасность политической коммуникации, в частности, гарантии-

руют беспроблемное и ненасильственное протекание процессов социальной трансформации, становление параметров правового государства и демократического гражданского общества

Во второй главе «Информационная безопасность политической коммуникации в современной России: содержание и приоритеты обеспечения», состоящей из трех параграфов, анализируются основные способы обеспечения информационной безопасности, направления государственной политики по оптимизации информационной безопасности политической коммуникации, а также концептуальная модель региональной системы информационной безопасности на примере информационной войны, охватывающей территорию Северного Кавказа

В первом параграфе второй главы «Способы обеспечения информационной безопасности политической коммуникации российского общества» рассматриваются пути и способы обеспечения информационной безопасности политических коммуникаций

Основные способы реализации информационной безопасности политической коммуникации государства получили свое отражение в научно обоснованной доктрине информационной безопасности Доктрина информационной безопасности государства является не только системой официально принятых взглядов по информационным и другим вопросам, но, прежде всего, руководством к действию На основе доктринальных положений осуществляется широкий круг политических мероприятий и действий во внешней и внутренней политике государства

Основными способами обеспечения информационной безопасности могут быть

- выработка согласованных политических, правовых, организационных и иных мер по обеспечению информационной безопасности государства,
- подготовка и реализация межведомственных программ, положений, инструкций и других нормативных актов, регламентирующих деятельность структур информационной организации государства,
- ликвидация дублирования функций тех или иных министерств и ведомств, их региональных структур,
- создание условий для повышения эффективности управления силами и средствами субъектов, участвующих в защите информационного пространства в интересах обеспечения информационной безопасности государства

Мировой опыт свидетельствует, что рациональная стратегия обеспечения информационной безопасности должна основываться на долгосрочных планах, учитывающих характер внешних и внутренних информационных угроз, приоритетах по обеспечению информационной безопасности государства и реальных экономических возможностях

Защита информационного пространства в России должна исходить не только из текущих возможностей, но и из перспективных потребностей обеспечения информационной безопасности государства Кроме того, эффективное функционирование информационной организации государства предполагает наличие четко отлаженной системы принятия и реализации согласованных решений, касающихся ее вопросов В противном случае информационная политика может вырабатываться узким кругом лиц без должного прогнозирования и всестороннего обоснования, определяться только сложностями нынешней политической и экономической ситуации, что может обострить существующие проблемы и в перспективе привести к крупным политическим, экономическим и социальным просчетам

Однако до сих пор в стратегическом планировании развития компонентов информационной организации политической коммуникации, к сожалению, нет четкого представления о принципах, путях и подходах, которыми следует руководствоваться при формировании и практической реализации информационной политики России

Такие сложные и жизненно важные элементы структуры государства, как мультисервисная сеть передачи данных, государственная сеть связи, Интернет-порталы органов государственной власти, электронные архивы, библиотеки и хранилища данных и др , не могут нормально функционировать, ориентируясь лишь на текущие проблемы Их развитие гораздо шире, а защита - первостепенная задача

В работе указывается, что обеспечение информационной безопасности исключительно средствами организационно-политического и нормативно-правового характера без создания эффективно функционирующей технической системы защиты информационного пространства страны невозможно обеспечить надежную безопасность политической коммуникации современного российского государства Иными словами, защита систем государственного управления на федеральном и региональном уровнях от несанкционированного воздействия на эти системы с целью причинения негативного

информационного ущерба органам государственной власти и управления должна иметь в качестве своего технического основания отлаженный механизм, способный противостоять информационным диверсиям

Таковым механизмом защиты информационной сферы политической коммуникации от несанкционированного воздействия должны стать информационный «щит» и «фильтр» Под «фильтром» понимаются маршрутизаторы и специальные программы, которые блокируют свободный поток информации В свою очередь информационный «щит» (в Китае его называют «Золотым щитом») представляет собой масштабный брандмауэр – виртуальное подобие «великой стены», предназначенный для постоянного и возможно полного контроля над несанкционированными информационными потоками

Во втором параграфе второй главы «Направления оптимизации политики в сфере информационной безопасности политической коммуникации современной России» представлен анализ приоритетных направлений обеспечения информационной безопасности политической коммуникации в современной России

Закономерностью политической жизни в условиях глобализации является резкое обострение информационного противоборства и, как следствие, информационных угроз для безопасности личности, общества и государства во всех сферах общественной жизни В этом контексте под политикой обеспечения информационной безопасности политической коммуникации понимается целенаправленная деятельность государства и политических институтов общества по выявлению, предупреждению и устранению угроз безопасности личности, обществу и государству в информационной сфере

К важнейшим направлениям оптимизации государственной политики в сфере информационной безопасности следует отнести эффективное прогнозирование и определение состояния современных угроз, опасностей и рисков информационной направленности, в частности, касающихся, информационного терроризма, развитие доктринальных основ информационной безопасности и ее места в общей системе безопасности современной России, развитие и систематическое совершенствование правовых основ обеспечения информационной безопасности России

К числу приоритетных задач оптимизации государственной политики в сфере информационной безопасности в современной России в работе отнесены

• совершенствование государственной политики в области обеспечения информационной безопасности Российской Федерации,

• разработка федеральных целевых программ обеспечения информационной безопасности,

• совершенствование правового, методического, научно-технического и организационного обеспечения информационной безопасности,

• усиление координации деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской федерации,

• расширение межгосударственного сотрудничества стран участниц ОДКБ по обеспечению информационной безопасности и д р

Особое место в комплексе приоритетных направлений государственной политики в сфере информационной безопасности в настоящее время отводится задаче обеспечения информационной безопасности государства в избирательных компаниях Это, пожалуй, самый главный вопрос, так как речь идет о качестве политической власти, которую будет создавать народ, и о том, как эта власть будет служить народу Обеспечение этой безопасности сегодня важнее, чем способность защититься от всех других видов оружия, от самых различных угроз Обеспечение информационной безопасности в избирательных компаниях - задача всех ветвей власти, органов местного самоуправления, всех патриотических политических партий, общественных объединений Выполнение этой задачи неотложно

Условием успешности государственной политики России в области использования и развития сетевых средств массовой коммуникации как одного из каналов политической коммуникации является необходимость учета не только социального, экономического, политического и культурного своеобразие нашей страны, но и особенности отечественных сетевых средств массовой коммуникации Сетевые средства массовой коммуникации в России имеют ограниченную базу для дальнейшего распространения Речь идет, прежде всего, о недостаточно разветвленной и качественной телефонной сети, а также о сравнительно небольшом компьютерном парке, однако с каждым годом положение меняется, появление сотовых и беспроводных технологий дает возможность доступа к сети Интернет в любой точке покрытия

В работе также обосновывается положение о том, что в интересах усиления информационной безопасности в России должна осуществляться адекватная социальным вызовам общества, государства и личности эффективная образовательная политика

В третьем параграфе второй главы «Концептуальная модель региональной системы информационной безопасности на Северном Кавказе» уточнены содержательные компоненты возможной концептуальной модели региональной системы информационной безопасности

В условиях социально-экономических и общественно-политических преобразований в России определяющая роль в формировании и реализации информационной политики принадлежит органам государственной власти, выступающим одновременно в качестве ее субъекта и объекта

Являясь органической частью системы обеспечения национальной безопасности, ее подсистемой, региональная информационная безопасность политической коммуникации, обеспечивается в соответствии с российским законодательством и учетом федеративной формы политико-территориальной организации государства

Структура региональной системы информационной безопасности (РСИБ), которую возглавляет Комиссия по информационной безопасности при главе администрации субъекта ЮФО, - орган, работающий на коллегиальной основе Обеспечение информационной безопасности в пределах своей компетенции осуществляют все органы государственной власти, местного самоуправления, предприятия, учреждения и организации региона

Ее системными элементами могут быть органы управления системой (Комиссия по информационной безопасности при администрации субъекта ЮФО, ее структурные подразделения), федеральные органы исполнительной власти, решающие общесистемные задачи региональной системы информационной безопасности на северном Кавказе, а также объектные (целевые) и функциональные подсистемы

Важнейшими организационными элементами РСИБ, решающими общесистемные задачи информационной безопасности, являются территориальные органы Гостехкомиссии России, Федеральной службы безопасности, Федеральной - службы охраны, Министерства внутренних дел Российской Федерации, которые имеют специфические функции и действуют в пределах их компетенции

К объектным (целевым) подсистемам РСИБ относятся системы информационной безопасности предприятий, учреждений и организации, расположенных на территории Субъектов Российской Федерации, имеющих объекты защиты Прежде всего, к ним относятся системы информационной безопасности предприятий регионального подчинения и предприятий вневедомственной принадлежности К ним также могут относиться подсистемы информационной безопасности федеральных органов исполнительной власти (подсистемы министерств и ведомств), расположенные на территории Субъекта Российской Федерации Объектные подсистемы имеют конкретные цели и объекты защиты, и используют специфические способы и средства информационной безопасности Деятельность этих подсистем носит комплексный характер и направлена на защиту объектов, находящихся в их ведении

К функциональным подсистемам РСИБ относятся подсистемы, реализующие отдельные функции обеспечения защитой информации К ним относятся подсистемы

- управления,
- защиты информационно-кибернетического пространства,
- защиты информационно-психологического пространства,
- кадрового и научного обеспечения информационной безопасности,
- сопутствующие функциональные подсистемы (оказание услуг и пр)

Объектные подсистемы РСИБ (системы информационной безопасности предприятий, учреждений и организаций), в свою очередь, могут содержать в своем составе собственные органы управления объектные и функциональные подсистемы информационной безопасности, предназначенные для непосредственного выполнения и обеспечения функций органов информационной безопасности на конкретных объектах защиты

В **Заключении** подведены итоги исследования и предложены рекомендации по оптимизации государственной политики в сфере обеспечения информационной безопасности политической коммуникации в Российской Федерации

В частности, указывается, что информационная безопасность политической коммуникации представляет собой такое состояние институтов государства и общества, при котором обеспечивается надежная защита национальных интересов страны и ее населения в информационной сфере При этом обязанность обеспечения информационной безопасности возлагается на информационную организацию государства как неотъемлемую часть систе-

мы национальной безопасности Построение надежной и оптимальной новейшим вызовам и угрозам российской государственности системы информационной безопасности - единственно возможный путь динамического развития России в XXI столетии

III. ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ ОТРАЖЕНО В СЛЕДУЮЩИХ ПУБЛИКАЦИЯХ:

1 Проценко Е В ,Чагилов В Р Проблемы трансформации политики в условиях информационного общества // Социально-гуманитарные знания – 2008 – №11 – С 156-164

2 Проценко, Е В Информация и ее безопасность в современном политическом пространстве // Студенческая наука – экономике города Невинномысска материалы V городской научно-практической конференции – Невинномысск Изд-во НГГТИ – 2006 – С 49-54

3 Проценко Е В Политические Интернет – технологии и их применение в современной России // Проблемы современного общества и мирового социума глазами молодежи материалы региональной студенческой конференции – Ставрополь Изд-во СевКавГТУ – 2006 – С 145-147

4 Проценко Е В Факторы государственной информационной политики в контексте современных коммуникационных процессов // Социальная эволюция, идентичность и коммуникация в XXI веке материалы региональной научно-практической конференции – Ставрополь Изд-во СевКавГТУ – 2007 – С 263-269

5 Проценко Е В Роль информационной безопасности в современном политическом пространстве РФ // Проблемы обеспечения национальной безопасности, гражданского мира и согласия в контексте глобализационных вызовов и угроз постсовременности материалы Международной научно-практической конференции – Невинномысск Изд-во НГГТИ – 2007 – С 241-246

6 Проценко Е В Информационное оружие как средство и способ ведения информационно-психологической войны // Молодежь и наука реальность и будущее материалы Международной научно-практической конференции – Т 2 – Невинномысск Изд-во НИЭУП – 2008 – С 285-289

Подписано в печать 03 07 2009

Формат 60x84 1/1	Усл печ л 1,36	Уч -изд л 1,2
Бумага офисная	Тираж 100 экз	Заказ 286

Отпечатано в Издательско-полиграфическом комплексе
Ставропольского государственного университета
355009, Ставрополь, ул Пушкина, 1