РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ

На правах рукописи

Молодчая Екатерина Николаевна

ПОЛИТИКА ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ В СОВРЕМЕННОЙ РОССИИ: ПОЛИТОЛОГИЧЕСКИЙ АСПЕКТ

Специальность 23.00.02 – политические институты, процессы и технологии

Автореферат
диссертации на соискание ученой степени
кандидата политических наук

Москва – 2011

Диссертация выполнена на кафедре политологии и социальной политики ФГБОУ ВПО «Российский государственный социальный университет»

Научный руководитель:	доктор философских наук, профессор Авцинова Галина Ивановна
Официальные оппоненты:	доктор политических наук, профессор Сулакшин Степан Степанович кандидат политических наук Вилисов Максим Владимирович
Ведущая организация:	Российский государственный университет туризма и сервиса, кафедра истории и политологии

Защита состоится «28» декабря 2011 года в 14 часов на заседании Диссертационного совета Д 212.341.02 по историческим и политическим наукам в Российском государственном социальном университете по адресу: 129226, г. Москва, ул. Вильгельма Пика, д.4, корпус 2, зал заседаний диссертационных советов.

С диссертацией можно ознакомиться в научной библиотеке Российского государственного социального университета, расположенной по адресу: 129226, г. Москва, ул. Вильгельма Пика, д.4, строение 5.

Автореферат размещен на сайте ВАК: www.vak.ed.gov.ru

Автореферат размещен на сайте РГСУ www.rgsu.net

Автореферат разослан «26» ноября 2011 года

Ученый секретарь Диссертационного Совета
доктор философских наук, профессор Г.И. Авцинова

Актуальность темы исследования

Теоретическое и практическое значение исследования политики противодействия кибертерроризму вызвано необходимостью глубокого осмысления теоретико-методологических, организационных, политических основ разработки и реализации данного вида политики и определяется следующими обстоятельствами.

Во-первых, одним из главных факторов развития социально-политической системы является производство и использование информации. В современных условиях она играет ключевую роль в функционировании не только общественных и государственных институтов, но и жизнедеятельности каждого человека. Компьютеры и информационно-коммуникационные системы используются во всех сферах деятельности человека и государства. Это обеспечение национальной безопасности, предоставление государственных услуг в области здравоохранения, образования, ЖКХ, управления аэро- и железнодорожным транспортом, торговли, финансов, а также межличностного общения и др. Влияние глобальных сетей на социально-политическое развитие общества многогранно и противоречиво. С одной стороны, они способствуют развитию потенциала человека через компьютерные игры, обучающие и развлекательные программы, интерактивное телевидение, электронную прессу. Глобальные сети оказывают влияние на электоральное поведение субъектов политики, процесс организации и проведения избирательных кампаний, механизмы коммуницирования власти и общества, презентацию и отстаивание политическими акторами своих интересов. Модифицируя систему взаимоотношений и взаимодействия институтов гражданского общества и государства, глобальные сети способствуют формированию конструктивного диалога между ними. С другой стороны, стремительное развитие информационно-коммуникационной сферы привело к появлению новых видов преступлений - компьютерной преступности и компьютерного терроризма. От деятельности кибертеррористов в виртуальном пространстве могут пострадать

тысячи пользователей сетей, не только отдельные люди, но и целые государства. Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей. Современные террористические организации активно используют информационно-коммуникационные технологии, наряду с традиционными средствами. При этом время перехода от угрозы до реального акта кибертеррористов значительно уменьшается.

Во-вторых, актуальность исследования этого вида политики возрастает в условиях усложнения социальной структуры и политической жизни общества, что кардинально модифицирует каналы артикуляции и агрегирования интересов акторов социально-политического взаимодействия, создает опасность для формирования диаметрально противоположных подходов к оценке политических событий и процессов, решению конкретных задач, выбору социальных ориентиров, форм политической активности. Опасность деструктивных явлений усиливается в условиях падения уровня легитимности власти, доверия населения к политическим институтам в целом и политике властвующей элиты в частности. Эти и другие явления в какой-то мере инициируют кибертеррористическую деятельность, усиливая потенциал кибертерроризма как способа давления на власть, поскольку они нередко ведут к неустойчивости функционирования социально-политической системы, несогласованности действий и взаимодействий политических институтов и лиц, функции которых связанны с разработкой и реализацией политики противодействия этому явлению. Появление нового вида терроризма угрожает безопасности личности, общества и государства на всех уровнях политики, что и обусловливает необходимость его всестороннего изучения.

В-третьих, эффективность политики противодействия кибертерроризму зависит не только от устойчивости функционирования социально-политической системы, развитости контроля государства над процессами в виртуальном пространстве, соблюдения правовых норм в данном сегменте внутренней и внешней политики, развития правовой грамотности элиты и населения и т.д. Во

многом она обусловлена наличием у властвующей элиты и представителей специальных служб инструментария познания анализируемого феномена, что невозможно без его концептуального осмысления, расширения и обогащения методологической палитры за счет подходов, позволяющих наиболее полно изучить сущность и особенности нового вида терроризма, как явления политики.

Таким образом, теоретическая и практическая значимость, недостаточная разработанность в мировой и отечественной практике эффективных социально-политических и правовых механизмов противодействия кибертерроризму обусловливает необходимость концептуального осмысления этого феномена, анализа его сущности, особенностей и тенденций функционирования, поиска и обоснования путей его минимизации, осмысления роли государства в противодействии этому негативному явлению. Таковы причины, обусловившие выбор данной проблемы для целевого концептуального осмысления.

Степень научной разработанности темы. Те или иные аспекты данной проблематики исследованы в отечественной и зарубежной политологической, исторической, психологической, социологической, научной и публицистической литературе. Сложность и многогранность феномена кибертерроризма, комплексный характер выработки эффективных мер противодействия ему требуют междисциплинарного подхода и объясняют многообразие возможных ракурсов изучения. В научной литературе теоретическая разработка этого феномена стала активно осуществляться в конце 20 века.

В первую очередь необходимо назвать исследования, связанные с анализом информационного общества, пределов информационной свободы, правовых, социально-экономических и научно-технических аспектов обеспечения национальной безопасности и антитеррористической деятельности. Прежде всего, это работы В.Э. Багдасаряна, В.Н. Галатенко, Е.А. Ерофеева, О.А. Колобова, А.В. Крутских, В.А. Конявского, В.Н. Лопатина,

С.В. Лопаткина, Б.Н. Мирошникова, И. Морозова, В. Нерсесяна, С.С. Сулакшина, Ю.С. Уфимцева, В.П. Шерстюка, В.Н. Ясенева и др.[1].

Большой массив литературы посвящен анализу средств массовой информации в противодействии терроризму. Среди исследователей этого направления следует назвать Е.Л. Вартанову, М. Гельмана, А. Евдокимова, А.Н. Курбацкого, М.М. Назарова, И.Н. Панарина, В.Е. Бернатски, П. Вилкинсона, Л.Д. Мартина и др[2].

---

[1] См.: Багдасарян В.Э. Демографические тренды и национальная безопасность России // Мир и политика. 2010. – №7 (46); Багдасарян В.Э. Научится мыслить в парадигме войн нового типа // Научный эксперт. 2011; Галатенко В.Н. Информационная безопасность: практический подход. – М., 1998.; Колобов О.А, Ясенев В.Н. Информационная безопасность и антитеррористическая деятельность современного государства: проблемы правового регулирования и варианты их решений. – Н. Новгород, 2001; Конявский В.А., Лопаткин С.В. Компьютерная преступность. Т.I. – М., 2006; Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. – СПб., 2000; Мирошников Б.Н. Борьба с киберпреступлениями одна из составляющих информационной безопасности Российской Федерации [электронный ресурс] / Б.Н. Мирошников. URL: http//www.crime-research.ru/articles/Miroshl (дата обращения: 16.07.2010); Морозов И.Л. Пределы информационной свободы в российском киберпространстве: как смягчить столкновение интересов государства, гражданского общества, независимой науки? [электронный ресурс]. URL: http://morozov.vlz.ru/library/infsvob.htm (дата обращения 16.07.2010); Нерсесян В. Национальная безопасность и формирование информационного общества в России // Власть. 2003. – №9; Сулакшин С.С. Категория «безопасность»: от категориального смысла до государственного управления // Научный эксперт. 2010; Сулакшин С.С. Национальная безопасность страны и качество национального образования // Родная Ладога. 2010. – №4; Уфимцев Ю.С., Ерофеев Е.А. и др. Информационная безопасность России. – М., 2003; Цыгичко В.Н., Вотрин Д.С., Крутских А.В. и др. Информационное оружие – новый вызов информационной безопасности. – М., 2000; Шерстюк В.П. Проблемы правового обеспечения информационной безопасности в Российской Федерации // Право-Информация-Безопасность. Альманах российского юридического журнала. 2002. – №1.

[2] См.: Вартанова Е.Л. Современная медиаструктура. // СМИ в постсоветской России. – М., 2002; Гельман А. Русский способ (Терроризм и масс-медиа в третьем тысячелетии). – М., 2003; Евдокимов А. Средства массовой информации в противодействии терроризму. // Мировое сообщество против глобализации преступности и терроризма. – М.: «Международные отношения», 2002; Курбацкий А.Н. Роль СМИ в борьбе с международным терроризмом [электронный ресурс]. URL: http://www.economy.bsu.by/library.pdf (дата обращения:18.10.2010); Назаров М.М. Массовая коммуникация в современном мире: методология анализа и практика исследований. – М., 2003; Панарин И.Н. СМИ и терроризм [электронный ресурс]. URL: http://www.panarin.com (дата обращения: 18.10.2010); Biernatzki W. E. Terrorism and Mass Media. // Center for the Study of Communication and Culture. – London. 2002. Vol. 21. – N.1; Martin L.J. The Media's Role in international Terrorism [электронный ресурс]. URL: http://www.pegasus.cc.ucf.edu~surette/mediasrole.html (дата обращения: 18.10.2010); Wilkinson P. The Media and Terrorism: A Reassessment. // Terrorism and Political Violence. – London. 2001. Vol. 9. – N.2.

Фундаментальное значение в исследовании феномена терроризма и его новой формы - кибертерроризма имеют работы Г. Веймана, С.Вилсона, М. Конви, Ф. Коэна, М. Поллитта, П.С. Пробста [3].

Среди российских ученых анализ интересующей нас проблемы представлен в работах Г.К. Варданянца, В.А. Голубева, В. Ибрагимова, Д.Г. Малышенко, Е.А. Роговского, Е.В. Старостиной, Т. Л. Тропиной[4] и др. Важно, что в этих работах немало внимания уделено исследованию политики противодействия кибертерроризму как одной из приоритетных задач не только государства, но и общества, анализу оценок угроз киберпреступности и предложениям по их нейтрализации.

В условиях развития информационного общества кибертерроризм перерос рамки регионального и национального масштаба. Интерес исследователей к проблемам современного международного кибертерроризма и формам его проявления связан с изменившейся политической ситуацией в мире, возросшей активностью террористических организаций на

---

[3] См.: Пробст П. Терроризм после терактов 11 сентября 2001 г. - новые сферы конфликта [электронный ресурс]. URL: http://www.crime-research.ru/news/12.05.2004/146 (дата обращения: 16.10.2010); Cohen F. Terrorism and Cyberspace // Network Security, 2002, Vol.5; Convey M. Terrorist use of Internet and Fighting Back // Materials of the conference Cybersafety: Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities. Oxford, 2005; Pollitt M., CYBERTERRORISM – Fact or Fancy? FBI Laboratory [электронный ресурс]. URL: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html (дата обращения 08.05.2010); Weimann, G. How Modern Terrorism Uses the Internet. Release Date: March 2004 No. 116 [электронный ресурс]. URL: http://www.usip.org/pubs/specialreports/srl 16.html (дата обращения: 08.05.2010); Wilson C. Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress [электронный ресурс]. URL: http://www.fas.org/sgp/crs/terror/index.html (дата обращения: 08.05.2010).

[4] См.: Варданянц Г.К. Терроризм: диагностика и социальный контроль // Социс. 2005; Голубев В.А. Кибертерроризм как новая форма терроризма [электронный ресурс]. URL: http://www.crime-research.org/ (дата обращения: 27.09.2009); Ибрагимов В. Кибертерроризм в Интернете до и после 11 сентября 2001г.: оценка угроз и предложения по их нейтрализации // Компьютерная преступность и кибертерроризм: Сборник научных статей / Под ред. Голубева В.А., Ахтырской Н.Н. Запорожье, 2004; Малышенко Д.Г. Противодействие компьютерному терроризму – важнейшая задача современного общества и государства [электронный ресурс]. URL: http://www.crime-research.ru/analytics/malishenko (дата обращения: 05.02.2011); Роговский Е.А. Кибербезопасность и кибертерроризм // США – Канада. Экономика, политика, культура. 2003, – №8; Старостина Е.В., Фролов Д.Б. Защита от компьютерных преступлений и кибертерроризма. – М.: 2005; Тропина Т. Л. Киберпреступность и кибертерроризм [электронный ресурс]. URL: http://www.crime-research.ru/analytics/ (дата обращения: 05.02.2011).

международной арене, необходимостью объединения усилий представителей общественности и государственных институтов, правоохранительных органов, всех конструктивных сил разных политических ориентаций на национальном и мировом уровне в борьбе с этим злом. Интерес исследователей к проблемам международного кибертерроризма, борьбы с ним в условиях нового миропорядка отражен в трудах А.П. Бутенко, Н.Н. Даниленко, И.Д. Паутова, Е.Г. Сатановского, А.И. Смирнова, Д.Б. Фролова, В.С. Чугунова и др[5]. Обращение к трудам ученых, исследующих международный кибертерроризм, способствовало осмыслению такого важнейшего аспекта политики противодействия этому явлению, как разработка международной системы наиболее эффективных антитеррористических мер на мировом уровне.

В работах Р. Альдриха, Д. Аркилла, Д. Барлоу, Д. Вертона, Д. Ронфельда, Д. Штейна исследуется влияние массовых информационных процессов на появление новой формы терроризма в аспекте вступления развитых стран в информационное общество[6]. С.В. Бондаренко, С.А. Дятлов,

---

[5]См.: Бутенко А.П. Глобализация: сущность, современные проблемы // Социально-гуманитарные знания. 2002. – №3; Даниленко Н.Н. О проблеме терроризма в Российской Федерации // Мировое сообщество против глобализации преступности и терроризма. – М.: «Международные отношения», 2002; Паутов И.Д. Современный международный терроризм – глобальная угроза человечеству. – М.: МГУ, 2005; Сатановский Е.Г. Глобализация террора и ее последствия // Международная жизнь. 2001. – №9,10; Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности / А.И. Смирнов. – М.: Изд. «Парад». 2005; Фролов Д.Б. Информационная война как инструмент политического воздействия. Монография. – М., изд-во МИФИ, 2003; Чугунов В.С. Международный терроризм как инструмент глобального управления // Национальная безопасность и геополитика России. – М., 2001, – №8(25).

[6] См.: Aldrich, Richard W. Cyberterrorism and Computer Crimes: Issues Surrounding the Establishment of an International Legal Regime / Richard W. Aldrich. Colorado: USAF Institute for National Security Studies, 2000; Arquilla J., Ronfeldt D. In Athena's Camp: Preparing for Conflict in the Information Age [электронный ресурс]. URL: http://www.au.af.mil/au/soc/athena.htm (дата обращения: 05.02.2011); Dr.J.Barlow. Netwar [электронный ресурс]. URL: http://bcis.pacificu.edu/journal/2001/10/editorial10.php (дата обращения: 05.02.2011); Stein G. J. Information War - Cyberwar – Netwar [электронный ресурс]. URL: http://www.airpower.maxwell.af.mil/airchronicles/battle/chp6.html (дата обращения: 05.02.2011); Verton D. Black Ice: The Invisible Threat of Cyber-Terrorism / D. Verton. Osborne: McGraw-Hill, 2003.

В.Г. Матюхин, А.В. Монойло, Д.Б. Фролов[7] исследуют данную проблему в контексте российского социально-политического процесса.

Зарубежные авторы М.Вайн, Д.Деннинг, Л. Жанзевски, Б. Колин, М. Конвей, Д. Левис, Т.Л. Томас, Д. Шиндер[8]; отечественные Г., Почепцов, С.Супиченко, А. Тихонов, М.П.Требин, А.В. Федоров[9] анализируют активную деятельность террористических групп в киберпространстве и сети Интернет, возможные каналы их финансирования и меры противодействия им.

На авторские выводы об источниках, особенностях, тенденциях развития кибертерроризма оказали влияние исследования в области проблем

---

[7] См.: Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Информационная безопасность. Учебное пособие. Учебное пособие под ред. В.Г. Матюхина для студентов ВУЗов, обучающихся по специальностям в области информационной безопасности. МГФ «Знание», 2005; Бондаренко С.В. Информационное общество. 2002, – №1; Дятлов С.А. Принципы информационного общества. Информационное общество. 2000, – №2; Матюхин В.Г. Информационно-технологическая инфраструктура предоставления государственных услуг населению и организациям как неотъемлемая компонента «электронного государства». Материалы Российского научно-экономического собрания. – М., 2007; Монойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. – М., 2003.

[8] См.: Denning D.E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy [электронный ресурс]. URL: http://www.nautilus.org/info-policy/workshop/papers/denning.html (дата обращения: 05.02.2011); Collin B. C. The Future of CyberTerrorism, Proceedings of 11th Annual International Symposium on Criminal Justice Issues, The University of Illinois at Chicago [электронный ресурс]. URL: http://www.acsp.uic.edu/OICJ/CONFS/terror02.htm (дата обращения 16.10.2010); Convey M. Terrorist use of Internet and Fighting Back. // Materials of the conference Cybersafety: Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities. Oxford., 2005; Janczewski L. Cyber Warfare and Cyber Terrorism / L.J. Janczewski. IGI Global, 2007. Lewis J.A. Assessing the Risks of Cyber Terrorism, Cyber War and other Cyber Threats [электронный ресурс]. URL:http://www.crimevl.ru//docs/stats/stat_82.htm (дата обращения: 16.10.2010); Thomas T.L. Al Qaeda and the Internet: The Danger of "Cyberplanning" [электронный ресурс]. URL: http://www.iwar.org.uk/cyberterror/resources /cyberplanning/al-qaeda.htm (дата обращения: 16.10.2010); Shinder D. Scene of Cybercrime: Computer Forensics Handbook [электронный ресурс]. URL: http://www.crimevl.ru.docs/stats/stat_97.htm (дата обращения: 16.10.2010); Whine M. Cyberspace: A New Medium for Communication, Command and Control by Extremists [электронный ресурс]. URL:http://www.ict.org.il/ (дата обращения: 08.05.2010).

[9] См.: Почепцов Г. Пока не начался джаз: терроризм как информационная технология особого типа [электронный ресурс]. URL: http://www.telegrafua.com; Супиченко С. Интернет экстремизм и терроризм/ С. Супиченко. – Информационно-аналитический журнал ЦАТУ: Ассиметричные угрозы и конфликты низкой интенсивности. – № 5. 2008; Тихонов А. Угрозы из киберпространства // Красная звезда от 08.08.2007; Требин М.П. Терроризм в XXI веке. –Минск, 2003; Федоров А.В. Супертерроризм: новый вызов нового века. – М., 2002.

информационного терроризма и кибервойны, представленные в монографиях и статьях И. Ю. Алексеева, И.И. Завадского, В.Г. Крысько, В.А. Лисичкина, Г.Г. Почепцова, С.П. Расторгуева, А. К. Рудакова, Г. Смоляна, В. Черного, С. Чугунова, Л. Шелепина и др.[10]

Правовая база борьбы с кибертерроризмом – важнейшее направление исследования политики противодействия этому явлению. Антитеррористическое и информационное законодательство России и зарубежных стран анализируется в работах В.Ф Антипенко, И.Л. Бачило, Н.И. Бусленко, В.Н. Лопатина, Ю.Н. Прусакова, Д. Свантессона, М.А. Федотова, Т.Л. Тропиной, С. Хаботина[11] и др.

Вклад в изучение феномена радикализма, экстремизма, терроризма, разработку направлений политики противодействия терроризму внесли работы ученых РГСУ Г.И. Авциновой, О.А. Белькова[12]. В указанных публикациях

---

[10] См.: Алексеев И.Ю. Информационные вызовы национальной международной безопасности. – М., 2001; Завадский И.И. Информационная война – что это такое? //Защита информации. Конфидент. 1996. № 4; Крысько В.Г. Секреты психологической войны (цели, задачи, методы, формы). – Минск, 1999; Лисичкин В.А., Шелепин Л.А. Третья мировая «информационно-психологическая» война. – М., 1999; Расторгуев С.П. Философия информационной войны. – М., 2001; Почепцов Г.Г. Информационные войны. – М.: Рефл-бук; К.: Ваклер, 2000; Смолян Г.Л. Новые технологии информационного воздействия на индивидуальное, групповое и массовое сознание // Проблемы психологии и эргономики. 2001. – №3; Черный В. Кибервойна за чужой счет // Национальная безопасность и геополитика России. – М., 2001. – №8 (25).

[11] См.: Антипенко В. Ф. Институциональный механизм борьбы с терроризмом: формирование правовой базы // Государство и право. 2004. – №11; Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник / Под ред. акад. РАН Б.Н. Топорнина. – СПб.: «Юридический центр Пресс», 2001; Бусленко Н.И. Политико-правовые основы обеспечения информационной безопасности РФ в условиях демократических реформ. Дис. д-ра полит. наук. – Ростов н/Д., 2003; Бусленко Н.И., Прусаков Ю.Н. Государственное обеспечение информационной безопасности России. – Ростов н/Д., 2002; Тропина Т.Л. Европейское законодательство о киберпреступлениях [электронный ресурс]. URL: http//crime.vl.ru/docs/stats/stat_110.htm (дата обращения: 12.08.2011); Хаботин С. Стратегия Великобритании в борьбе с терроризмом [электронный ресурс]. URL: http//www.agentura.ru/dossier/uk (дата обращения:10.12.2010); Svantesson Dan Jerker B. Private international law and the internet. Kluwer Law International, 2007.

[12] См.: Авцинова Г.И. Политический радикализм в России: социокультурный аспект. – Киев, 1995; Авцинова Г.И. Политический радикализм в России: концептуальные подходы к анализу и пути нейтрализации // Вестник МГУ. Серия 12. Политические науки, 1995, № 3,4; Авцинова Г.И. Статьи по социальной революции, радикализму, анархо-синдикализму, гегемонизму, экстремизму в политической энциклопедии. В 2-х томах. – М., 1999; Авцинова Г.И. Мировое сообщество в процессе глобализации и политические стратегии России //

дается анализ истоков терроризма, концептуальных подходов к изучению этого явления, путей нейтрализации влияния на политические процессы, тенденций информационной войны против России.

Значительный вклад в осмысление феномена кибертерроризма, разработку политики противодействия ему вносят специалисты профильных учреждений и ведомств России, в частности, ФСБ, МВД, МИД, МЧС, Военного университета и др. Особо следует отметить исследования Центра проблемного анализа и государственно-управленческого проектирования[13].

Терроризм и кибертерроризм анализируется в ряде диссертационных работ. Следует назвать диссертации Аксеновой С.В., Зарубина С.В., Илюшина Д.А., Паутова И.Д., Таран А.В., Тропиной Т.Л., Фролова Д.Б., Шагинян Г.А. и др[14]. Отмечая вклад указанных авторов в исследование различных аспектов терроризма вообще и кибертерроризма в частности, следует отметить, что

Ученые записки РГСУ. 2004. – № 2 (40); Авцинова Г.И. Тенденции информационной войны против России // Обозреватель - Observer. 2011. – №7;Авцинова Г.И. Перспективы и грани сотрудничества России, Индии и Китая в решении демографических проблем и осуществлении политики противодействия международному терроризму // Россия, Индия, Китай: состояние и перспективы геополитического и социально-экономического сотрудничества. Материалы круглого стола. – М.: РГСУ, 2009; Бельков О.А. Международный терроризм – слова и смыслы // Власть. 2002. – № 2; Бельков О.А. К философии терроризма и борьбы с ним // Власть. 2004. – № 7.

[13] Национальная безопасность: научное и государственное управленческое содержание. Материалы Всероссийской научной конференции. – М.: Научный эксперт, 2010; Россия в мире: гуманитарное, политическое и экономическое измерение. Материалы Всероссийской научной конференции. – М.: Научный эксперт, 2010; Информационная война против Российской Федерации. – М.: Научный эксперт, 2011.

[14] См.: Аксенова С.В. Политика противодействия терроризму в современной России. Дис.канд.полит.наук. – М., 2006; Зарубин С.В. Разработка алгоритмов и моделей противодействия кибертерроризму: дис.канд.техн.наук: 05.13.18,05.13.18,05.13.19. – Воронеж, 2009; Илюшин Д.А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг интернет: дис.канд.юрид.наук: 12.00.09. – Волгоград, 2008; Паутов И.Д. Международный терроризм в конце XX – начале XXI веков, как глобальная проблема современности: сущность, истоки и угрозы: дис.канд.полит.наук: 23.00.04. – М., 2006; Таран А.В. Международный терроризм как политический феномен. Проблемы антитеррористической борьбы: дис.канд.полит.наук: 23.00.04. – М., 2009; Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис.канд.юрид.наук: 12.00.08. – Владивосток, 2005; Фролов Д.Б. Информационное противоборство в сфере геополитических отношений: дис.канд.филол.наук: 10.01.10. – М., 2006; Шагинян Г.А. Антитеррористическая информационная политика Российского государства: дис.канд.полит.наук: 23.00.02. – Краснодар, 2006.

вопросы эффективной государственной политики противодействия этому явлению изучены недостаточно.

Автор обращался к нормативно-правовым документам, федеральным законам Российской Федерации. Среди них важное значение имеют Федеральные законы «Об информации, информатизации и защите информации», «О средствах массовой информации», «О связи», «О безопасности», «О борьбе с терроризмом». Большую помощь в анализе антитеррористической политики государства оказали Доктрина информационной безопасности Российской Федерации, Стратегия развития информационного общества в Российской Федерации и Стратегия национальной безопасности Российской Федерации до 2020 года.

Таким образом, анализ литературы по тематике диссертации показал, что в зарубежной и отечественной науке создана научная база для дальнейшего, углубленного анализа этой новой разновидности терроризма. Однако исследователи нередко акцентируют внимание лишь на отдельных аспектах, проявлениях, причинах активизации кибертерроризма. Практические рекомендации по минимизации его распространения и воздействия на общество часто носят сегментарный характер. Между тем масштабы распространения и последствия от кибертеррористических актов диктуют необходимость более углубленного политологического анализа угроз кибертерроризма, разработки и осуществления эффективной антитеррористической политики государства.

Объектом исследования является кибертерроризм как социально-политический феномен и политика противодействия ему.

Предметом исследования является анализ социально-политических причин, факторов, детерминирующих возрастание угрозы кибертерроризма, тенденций и особенностей его функционирования, выявление противоречий, влияющих на процесс разработки и реализации политики противодействия кибертерроризму в современной России.

Цель исследования заключается в изучении приоритетных направлений государственной политики противодействия этому виду

терроризма, выработке рекомендаций по предупреждению актов кибертерроризма, совершенствованию стратегии борьбы с этим негативным явлением с учетом российского и зарубежного опыта.

Цель исследования определила необходимость решения следующих **теоретических и эмпирических задач**:

1. Систематизировать основные научные подходы к изучению феномена кибертерроризма.
2. Проанализировать понятие «кибертерроризм», дать его авторское определение как социально-политического явления.
3. Выявить политические, социальные, экономические и другие причины возникновения и активизации кибертерроризма на современном этапе, его особенности и тенденции функционирования.
4. Выявить противоречия, влияющие на процесс разработки и реализации государственной политики противодействия кибертерроризму.
5. Проанализировать международный опыт противодействия кибертерроризму, выявить его значение для разработки и эффективной реализации данного вида политики в современной России.
6. Исследовать приоритетные направления деятельности российского государства в вопросах противодействия кибертерроризму и использования сети Интернет террористическими организациями;
7. Дать оценку эффективности деятельности государства в данном сегменте политики, разработать рекомендации по совершенствованию государственной политики противодействия этому явлению.

Гипотеза исследования. Автор исходит из научного предположения о том, что такая относительно новая разновидность терроризма, как кибертерроризм, в XXI веке имеет тенденцию к распространению. Его угроза существенно возрастает в связи с повсеместным развитием глобальных сетей и недостаточным развитием правового и иного контроля государства, а также в период политических и социально-экономических трансформаций. Однако и в

стабильных социально-политических системах возможна активация кибертеррористической деятельности. Повышение эффективности государственной политики противодействия кибертерроризму потребует его комплексного исследования, объединения усилий государственных институтов и структур гражданского общества, ранней диагностики его угроз, развития правовых основ и культуры, комплекса превентивных мер.

Теоретико-методологическая основа исследования

Методологическую основу исследования составили концептуальные положения институциональной теории, теорий «вызов-ответ», информационного и сетевого общества.

В исследовании использовались методы политологического, исторического, системного, сравнительного, статистического анализа, классификации, систематизации, обобщения, описания, а также критической интерпретации фактов, явлений, процессов. Совокупность данных методов позволила автору всесторонне подойти к изучению такого сложного феномена, как кибертерроризм, выявить его специфику среди других социально опасных явлений и определить приоритетные направления противодействия ему.

Источниковую и эмпирическую базу исследования составили нормативно-правовые документы разных стран и международных организаций. В работе использованы нормативно-правовые акты, а именно законы Российской Федерации, указы, постановления и распоряжения Президента РФ и Правительства РФ, в том числе международные конвенции и декларации, регулирующие основные направления развития политики противодействия кибертерроризму, программные политические документы, информационные материалы конференций и тематических круглых столов, политическая публицистика. Эмпирическую базу исследования составили данные социологических исследований, проведенных ВЦИОМ, Аналитическим Центром Юрия Левады, центром РОМИР-мониторинг, Центром проблемного анализа и государственно-управленческого проектирования, а также результаты авторского социального опроса.

Научная новизна диссертации состоит в следующем:

1. В политологическом контексте проанализированы сущность, причины возникновения и тенденции развития кибертерроризма.

2. Систематизированы и изучены парадигмы возможного анализа кибертерроризма как социально-политического феномена, предложено авторское определение понятия «кибертерроризм».

3. Выявлены противоречия в реализации государственной политики противодействия кибертерроризму в современной России.

4. Проведен анализ приоритетных направлений государственной политики противодействия кибертерроризму на основе зарубежного и российского опыта.

5. Предложены новые государственно-управленческие решения для повышения эффективности государственной политики России в противодействии кибертерроризму.

Основные положения, выносимые на защиту:

1. Кибертерроризм – это многогранный феномен, обусловленный во многом бесконтрольным использованием глобальных сетей, недостаточным вниманием со стороны государства, гражданского общества и спецслужб к данному сегменту политики, проявляющийся в атаках на компьютеры, компьютерные программы и сети или находящуюся в них информацию, с целью создания атмосферы страха и безысходности в обществе во имя достижения целей и интересов субъектов террористической деятельности, требующий объединения усилий мирового сообщества для эффективного противодействия ему.

2. Проблема обеспечения безопасности компьютерной информации и технологий является сегодня одной из самых острых для большинства стран мира. В первую очередь это касается использования информационных систем и сетей в государственном управлении, военной и промышленной сферах, бизнесе. Разработка эффективной политики противодействия кибертерроризму

ведется по следующим основным направлениям: определение приоритетных целей (глобальные, региональные, национальные) и средств (ресурсов), выявление возможных кибертеррористических угроз, защита населения, создание и координация международной инфраструктуры противодействия кибератакам, включающей в себя разработку специальных антитеррористических программ, норм международного права и др.

3. Обеспечение безопасности от кибертеррористической угрозы становится одним из главных приоритетов национальной безопасности России. Государство осуществляет политику противодействия кибертерроризму в рамках реализации основных принципов построения информационного общества. Это обусловлено необходимостью создания общенациональных систем безопасности информационно-коммуникационной инфраструктуры, обеспечивающих надежную ее защиту от возможных угроз.

4. В противодействии кибертерроризму приоритетное значение должно принадлежать оперативному пресечению кибертеррористических атак на стадии их подготовки (анализ информации, разработка законов, контроль со стороны государства), а также проведению на постоянной основе мониторинга состояния информационно-коммуникационного пространства, донесению необходимой информации до населения, профилактической работе (воспитательная, правовая, организационная) и др. Перечисленные меры должны всегда находится в центре внимания федеральной и региональной власти. Пролонгация кибертеррористических атак в повседневную жизнедеятельность социума обусловила необходимость разработки различных программ и мероприятий по организации разнообразной помощи жителям, пострадавшим от кибертеррористических действий, минимизации наносимого ущерба.

5. Механизмы политического регулирования в сфере государственной политики противодействия кибертерроризму предполагают учет таких факторов, как наличие у власти экономических, технических, правовых, организационных и иных ресурсов, которые необходимо

задействовать в процессе реализации антитеррористических акций и программ, уровень ответственности граждан, характер освещения данной проблемы в СМИ, последствий совершения кибератак, уровень использования других компьютерных сетей, анализ сайтов, состояние систем защиты собственных сетей, а также объектов повышенной опасности и др.

6. В 2008 и 2011 гг. автором проведено исследование, целью которого было выявить мнение населения (студенты ВУЗов и специалисты ИТ) об эффективности государственной политики противодействия кибертерроризму. Было опрошено 800 человек. Исследование показало низкую информированность респондентов об исследуемом явлении, наличие не полной и не всегда достоверной информации о данном явлении, необходимость институционализации профилактической работы государства и спецслужб в качестве ведущего направления политики противодействия этому явлению.

Теоретическая значимость диссертации. Проведенное исследование, дополняя имеющиеся по этой проблеме работы, расширяет возможности дальнейшего изучения сущности, особенностей и тенденций функционирования этого феномена в политическом процессе России, углубляет представления о факторах, детерминирующих это явление, позволяет найти наиболее эффективные пути минимизации последствий воздействия кибертерроризма на социально-политическую систему, деятельность власти и общества.

Практическая значимость диссертации заключается в том, что полученные теоретические выводы и рекомендации могут содействовать повышению эффективности практической деятельности органов государственной власти и силовых структур.

Научные результаты исследования могут быть также учтены при разработке современной доктрины безопасности РФ, дальнейшей разработке государственной политики противодействия кибертерроризму, выявлении наиболее эффективных направлений предупреждения и нейтрализации кибератак. Материалы диссертации могут использоваться для подготовки

учебных пособий и программ, преподавания спецкурсов в высшей школе, а также системе специальных учебных заведений.

Апробация работы. За период 2006-2011 годы автор участвовал в работе более 20 научных конференций. К наиболее значимым из них относятся: Глобальный форум по партнерству государств и бизнеса в противодействии терроризму (г. Москва, 2006 год), проводимый при участии МИД России; Конференция «Безопасность в информационном обществе» (г. Москва, 2011 год) при поддержке Министерства связи и массовых коммуникаций; круглые столы «Борьба с киберпреступностью в Интернете» и «Киберпреступность и Интернет. Вопросы защиты от противоправного контента» (г. Москва, 2011 год) в рамках Национального форума информационной безопасности «Инновационные решения для безопасности России»; Научная конференция «Россия в мире: гуманитарное, политическое и экономическое измерения» (г. Москва, 2010 год); Научно-исследовательский семинар «Россия 2030 глазами молодых ученых» (г. Москва, 2011 год) Центра проблемного анализа и государственно-управленческого проектирования.

Диссертация обсуждена на заседании кафедры политологии и социальной политики РГСУ и рекомендована к защите, протокол № «2» от 21 сентября 2011 года.

Структура диссертационного исследования. Диссертация состоит из введения, двух глав, содержащих 6 параграфов, заключения, списка использованных источников и литературы, приложения.

Основное содержание работы.

Во **введении** обосновывается актуальность темы диссертационного исследования, характеризуется степень изученности проблемы, формулируются объект, предмет, цель и задачи работы, определяется теоретико-методологическая основа исследования, анализируется его источниковая база, отмечается научная новизна, теоретическое и практическое значение диссертации, формулируются основные положения, выносимые на защиту.

В главе I «Теоретико-методологические основы исследования феномена кибертерроризма», состоящей из трех параграфов, автор рассматривает концептуальные основы изучения феномена кибертерроризма, выделяет парадигмы исследования, адекватные поставленным в диссертации целям и задачам, проводит анализ основных методологических подходов возможного исследования этого явления, дает определение кибертерроризма с учетом авторской трактовки в контексте развития информационного общества, выявляет причины возникновения и тенденции развития кибертерроризма.

Первый параграф **«Анализ понятия «кибертерроризм» в контексте политической науки»** посвящен изучению основных концептуальных подходов к исследованию феномена кибертерроризма.

Автор исходит из многогранности этого феномена, что обуславливает многообразие исследовательских подходов в анализе его сущности. На основе критического рассмотрения теорий вызов-ответ, информационного и сетевого общества, институциональной, функциональной, структурной и правовой парадигм возможного исследования кибертерроризма формулируются соответствующие принципы и критерии интерпретации его сущности и содержания. Рассматривая это явление в аспекте теории вызов-ответ кибертерроризм выступает в качестве вызова обществу, которое, в свою очередь, через проведение государственной политики противодействия ему отвечает на него. Опора на теорию информационного общества дает возможность более глубокого изучения сущности явления кибертерроризма и содержания государственной политики противодействия ему. Применительно к задачам нашего исследования теория сетевого общества является основой для анализа условий распространения кибертерроризма посредством глобальной сети Интернет и организации эффективной политики противодействия ему в связи с усложнением информационно-коммуникационной структуры государственного управления.

Отмечая достоинства и недостатки подходов изучения феномена кибертерроризма, автор приходит к выводу, что каждая из рассмотренных

парадигм содержит знание отдельных аспектов данного явления. Ни одна из них, используемая в отдельности от других, не достаточна для всестороннего изучения сущности и содержания кибертерроризма. По мнению автора, необходим комплексный подход, обусловленный многоаспектностью составляющих этот феномен явлений (киберпространство, терроризм, информационное общество, информатизация), а также противоречивостью и сложностью процессов, отражаемых этим понятием. Необходимо подчеркнуть, что выбранные в диссертации парадигмы не исключают поиск новых исследовательских моделей для изучения этого многогранного феномена.

Проведя сравнительный анализ понятия кибертерроризма, данного в других работах, автор приходит к выводу, что у исследователей нет единой трактовки в понимании сущности этого явления. Это во многом обусловлено тем, что каждый исследователь в определении кибертерроризма акцентирует внимание на различных его проявлениях в контексте тех задач, которые он определил, исходя из специфики той или иной науки. На наш взгляд, в определении этого понятия необходимо отметить глобальный характер угроз кибертерроризма, что обуславливает необходимость объединения усилий всего мирового сообщества для организации эффективного противодействия этому опасному явлению.

Во втором параграфе **«Причины возникновения и условия функционирования кибертерроризма в XXI веке»** автор останавливается на выявлении основных причин возникновения и активизации кибертерроризма.

К основным политическим причинам возникновения кибертерроризма можно отнести: усиление глобального цифрового противоборства и цифровой разрыв; военная агрессия в отношении другого государства и его оккупация; обострение внутриполитических конфликтов внутри самого государства; отсутствие эффективных механизмов взаимодействия государственной власти и гражданского общества; поощрение кибертерроризма на уровне государственной политики и др. К социальным причинам можно отнести: возросшую социальную дифференциацию, заметное снижение качества

жизненного уровня; замедленный процесс формирования среднего класса, как основы социальной стабильности и др. К экономическим причинам можно отнести: экономический и энергетический кризис, рост цен, инфляцию; раскол общества на группы с различным экономическим положением; отставание в развитии инновационной системы и использовании информационных и телекоммуникационных технологий и др.

В параграфе анализируются основные условия активизации кибертерроризма в аспекте использования уникальных возможностей Интернета для ведения кибертеористических атак. К ним относятся: свободный доступ к ресурсам глобальной сети; частичное и полное отсутствие регулирования, цензуры, контроля со стороны государства и общества; потенциально огромная аудитория во всем мире; анонимность связи; быстрое движение информации; невысокая стоимость создания сайта и обслуживания присутствия в сети; мультимедийная среда: возможность комбинировать текст, графику, аудио и видео и др. Это создает предпосылки расширения аудитории, использующей Интернет как источник информации.

В третьем параграфе **«Тенденции развития кибертерроризма»** автор анализирует переход мирового сообщества к информационному обществу, проблемы его формирования в России и влияние информационных технологий на политику государства и отмечает, что внедрение передовых информационно-коммуникационных технологий и систем, создает необходимые предпосылки для эффективного противодействия кибертерроризму. Автор обращает внимание на то, что постоянно растет взаимосвязь информационных и компьютерных систем, составляющих ядро инфраструктуры государства, подключенных к Интернету. Воздействию атак кибертеррористов подвергаются, в первую очередь, атомные реакторы, системы управления авиа и железнодорожным транспортом, крупные хранилищ стратегических видов сырья, распределения электроэнергии и водоснабжения, химические и биологические лаборатории.

В параграфе структурируются и характеризуются основные тенденции развития кибертерроризма как политико-социального явления, которые включают в себя: общий рост проявлений кибертерроризма, использование мирных технологий в качестве средств кибератак; использование кибертеррористами информационно-коммуникационных сетей и систем, посредством которых происходит воздействие на большие массы людей; создание развернутой инфраструктуры террористической деятельности в Интернете (сайты террористической направленности для пропаганды идей экстремизма, возможность постоянно поддерживать связь при помощи новейших мобильных устройств); использование в террористических акциях новейших достижений науки и техники в области компьютерных и информационных технологий; стремление кибертеррористов влиять на принятие государственных решений в целях ослабления деятельности правоохранительных органов, торможения законодательных инициатив, посредством насильственных методов.

В главе II **«Основные направления повышения эффективности государственной политики противодействия кибертерроризму в современной России»**, состоящей из 3 параграфов, автор исследует международный и российский опыт борьбы с кибертерроризмом, отмечает пути повышения эффективности государственной политики противодействия кибертерроризму.

В первом параграфе **«Противоречия в реализации политики противодействия кибертерроризму в современной России»** автор отмечает противоречивость обсуждаемых в обществе взглядов на необходимость или на отсутствие необходимости государственного регулирования национального сегмента сети Интернет. С одной стороны, реализация гражданином конституционных прав на свободное получение информации и пользование ею, и, с другой стороны, необходимость обеспечения безопасности государства, общества и личности в информационно-коммуникационной сфере. Использование террористами этих прав и свобод для пропаганды своей

деятельности, подрыва государственного строя и причинения иного ущерба, обусловливает необходимость безусловного обеспечения законности и правопорядка, стоящих на защите общества и личности, закрепления права за спецслужбами осуществлять мониторинг виртуального пространства и принятия мер к прекращению деятельности в нем террористических структур. На основе анализа нормативно-правовых документов, автор также выявил и другие политические, социальные и экономические противоречия в реализации государственной политики противодействия в России, воздействующие на характер и тенденции развития кибертерроризма. К этим противоречиям можно отнести: противоречие между основными участниками глобального информационного общества, на основе усиления глобального информационного противоборства; противоречие, обусловленное социальной деформацией общества, отток активной части населения из приоритетных сфер жизнедеятельности (производства, науки, образования) и др. В условиях ограниченных финансовых, материально-технических, ресурсных и иных возможностей они ведут к тяжелым социальным последствиям, создавая основу напряженности в обществе, и тем самым формируют социальную базу кибертерроризма.

Автор приходит к выводу о том, что отдельные непродуманные политические решения сами продуцируют кибертерроризм в стране. Указанные проблемы актуализируют необходимость осмысления существующих и выработке новых политико-правовых механизмов борьбы с кибертерроризмом. Компетенция специальных и правоохранительных органов в сфере предупреждения и пресечения кибертерроризма весьма ограничена с точки зрения возможного влияния на причины активизации и распространения этого опасного явления. Это диктует необходимость создания единой, отсутствующей сегодня в России, целостной, комплексной, стратегически ориентированной государственной концепции борьбы с кибертерроризмом, которая должна стать прочным фундаментом организации контртеррористической деятельности в стране. Таким образом, главными

субъектами борьбы с кибертерроризмом должны быть само государство, законодательная и исполнительная ветви власти.

Во втором параграфе **«Политика противодействия кибертерроризму: российский и международный опыт»** диссертации автор анализирует политику отдельных государств и возможности международного сотрудничества в сфере борьбы с кибертерроризмом. Параграф посвящен исследованию национальных программ и проектов, а также характеристике составных элементов инфраструктуры в борьбе с кибертерроризмом в различных странах (США, страны Западной Европы, Юго-восточной Азии, СНГ).

Военно-политическое руководство многих стран уделяет большое внимание развитию информационных технологий как одного из важнейших средств ведения военных действий в современных условиях. Растущая значимость информационной борьбы заставляет руководство государств активно прорабатывать вопросы адаптации и улучшения концепций ведения информационных операций.

Автор отмечает, что существуют наступательный и оборонительный типы политики противодействия угрозе кибертерроризма. Наступательная политика ведется преимущественно в западных странах (США, страны ЕС). Наращивание потенциала для ведения кибервойн свидетельствует о переходе этих стран к принципу «активной обороны», так как ранее основное внимание уделялось только вопросам обеспечения информационной безопасности. Выделение наступательной составляющей информационного противоборства в отдельную структуру, по оценкам западных экспертов, является адекватным ответом на существующие угрозы информационной безопасности. Автор отмечает, что многие страны развивают концепции ведения информационных войн. Они рассматривают киберпространство в качестве реального физического поля, охватывающего социальную, техническую (информационные системы и сети) и интеллектуальную (процессы обработки информации) сферы.

Ко второму типу реализации политики противодействия кибертерроризму относят страны Юго-Восточной Азии и СНГ. Эти государства отстают в сфере развития информационных технологий от наиболее развитых в военном и экономическом отношении стран. В настоящее время в этих странах практически отсутствуют: целостная нормативно-документальная система, регламентирующая организацию мероприятий, связанных с использованием информационных технологий при нарушении функционирования объектов информационной и телекоммуникационной инфраструктуры зарубежных государств; подразделения компьютерной разведки и контрразведки; антивирусная защита; кадровый потенциал. Это говорит об их неготовности в настоящее время к противодействию кибертерроризму и достижению информационного превосходства над противником. В этой связи руководство этих стран предполагает комплексное ускорение развития всех компонентов информационного противоборства, прежде всего в военной области (развития информационной инфраструктуры государства и технологий военного назначения, специальной подготовки личного состава). На сегодняшний день, главной задачей политики противодействия кибертерроризму в этих государствах является противодействие предполагаемой военной угрозе со стороны более развитых в этой сфере стран.

Проведенный теоретический анализ зарубежной политики противодействия кибертерроризму позволил автору выявить возможные направления повышения эффективности политики кибербезопасности в России, которые будут включать наступательные и оборонительные аспекты. К этим направлениям можно отнести: разработку основных направлений политики в сфере обеспечения национальной безопасности с учетом новейших информационных технологий; обеспечение стратегического информационно-коммуникационное доминирования, предполагающее постоянное развитие и внедрение инновационных информационных технологий; обеспечение надежного и устойчивого функционирования сетей и систем федерального и местных правительств; повышение эффективности взаимодействия

федеральных и региональных государственных структур в плане подготовки противодействия возможным кибертеррористическим атакам; отказ от использования иностранного программного обеспечения на объектах общенациональной информационно-технологической инфраструктуры; участие в международных переговорах и поддержание контактов с аналогичными структурами иностранных государств; совершенствование подготовки специалистов по кибербезопасности, которые должны владеть инструментами оборонительного и наступательного назначения и др.

В параграфе раскрываются важные мероприятия, проводимые российским государством по разработке основных положений в законодательстве в сфере защиты информационной среды и перехода к информационному обществу. Рассматривается процесс формирования и реализации российской государственной политики в области создания общенациональной информационно-технологической инфраструктуры, максимально учитывающей потребности государственного и военного сектора. По мнению автора, использование общенациональной информационно-технологической инфраструктуры «электронного государства» на основе единого национального пространства электронных идентификационных элементов позволит обеспечить высокую безопасность от угроз кибертерроризма.

Автор отмечает, что для организации эффективного противодействия кибертерроризму необходимо объединение усилий различных государств, их правоохранительных органов и специальных служб. Подобное взаимодействие возможно при условии, когда интересы различных государств в этой сфере совпадают, с учетом региональных и национальных особенностей законодательств. Это возможно в рамках двусторонних и многосторонних подходов к сотрудничеству. Автор рассматривает достоинства и ограниченность этих подходов, и, исходя из этого, формулирует задачи по защите информационно-коммуникационной инфраструктуры стран-союзников от кибертерроризма, которые включают в себя: разработку научно-

методического обеспечения по пресечению транснациональных (трансграничных) террористических атак с использованием глобальных информационных сетей, выработку единого понятийного аппарата, шкалу оценки киберугроз и их последствий; выработку механизмов взаимного информирования о широкомасштабных компьютерных атаках и крупных инцидентах в киберпространстве; выработку способов совместного реагирования на угрозы кибертерроризма; унификацию национальных законодательств в сфере защиты информационно-коммуникационной инфраструктуры от кибертерроризма и др.

Автор приходит к выводу о необходимости проведения регулярных встреч глав государств, руководителей специальных ведомств, экспертов с целью обмена опытом и информацией по этой проблеме; согласования единых позиций в оценке угроз и кибертеррористической деятельности; корректировки существующих законодательств в целях адекватного принятия мер против кибертеррористов.

Третий параграф **«Повышение эффективности политики противодействия кибертерроризму в России»** посвящен исследованию проблем оптимизации государственной политики в области противодействия кибертерроризму. Автор акцентирует внимание на том, что на современном этапе в целях обеспечения национально безопасности государства в сфере информационных технологий, а также устойчивого политического и социально-экономического развития страны в целом, необходимо совершенствование политики противодействия кибертерроризму.

Автор приходит к выводу о том, что российская система обеспечения безопасности от угроз кибертерроризма должна представлять собой многоуровневую иерархическую, территориально распределенную систему, в функции которой должны входить: анализ существующей структуры национальной безопасности государственной информационно-коммуникационной инфраструктуры; создание единой, комплексной стратегически ориентированной государственной концепции борьбы с этим

явлением; модернизация законодательства в сфере борьбы с терроризмом; взаимодействие всех сил правопорядка и спецслужб в антитеррористической борьбе с выделением головного органа, обладающего необходимыми полномочиями и правами в организации, координации и осуществлении всей борьбы с кибертерроризмом, и возложением на него ответственности за ее результативность; создание единой информационной системы, как в России, так и в рамках СНГ по вопросам борьбы с кибертерроризмом (распределенные банки данных с центральным информационным звеном на базе головного органа) и осуществление аналитической работы по вопросам основных угроз кибертерроризма; мониторинг угроз безопасности, состояния защищенности объектов информационно-коммуникационной структуры; отработка эффективных методов взаимодействия (информационных, совместных операций) с зарубежными органами, осуществляющими борьбу с кибертерроризмом; разработка правового механизма в осуществлении санкций против кибертеррористов, также для лиц связанных в той или иной форме с кибертеррористической деятельностью (передача финансовых, материальных и технических средств, обеспечение связи, недоносительство о фактах подготовки и проведения кибертеррористических актов, совершение подобных актов и т.д.), привлечения их к уголовной ответственности и др.

Автор выделяет некоторые приоритетные направления развития российской политики, которые создают основу для организации эффективного противодействия кибертерроризму. Эти направления включают в себя: присоединение России к международным договорам о противодействии кибертерроризму и кибервойне; активный переход к формированию информационного общества; развитие единого информационного пространства страны; развитие информационно-коммуникационной инфраструктуры; контроль над использованием информационных и телекоммуникационных технологий в государственном секторе; формирование эффективной стратегии инновационного развития страны; обеспечение информационной безопасности государства, общества, личности.

Решение этих важнейших общегосударственных задач имеет ключевое значение как для кардинального совершенствования системы государственного управления, так и для организации эффективного противодействия угрозам кибертерроризма.

Автор отмечает, что повышение эффективности борьбы с кибертерроризмом возможно лишь путем принятия всесторонних мер, которые будут в себя включать: четкую и последовательную политику, высококвалифицированную разведку, повышение качества работы правоохранительных органов и вооруженных сил, решение кадрового вопроса в создании ответственной команды профессионалов, а также технические средства предотвращения техногенного и кибернетического террора.

В заключении автор обобщает результаты исследования, формулирует выводы, дает практические рекомендации по проведению эффективной государственной политики противодействия кибертерроризму.

В **приложении** приведены результаты авторского исследования.

Основное содержание исследования отражено в следующих публикациях.

Публикации в журналах, рекомендованных ВАК:

1. Пахарева Е.Н. Кибертерроризм как технология воздействия на молодежную среду: причины и пути минимизации // Ученые записки Российского государственного социального университета. – М.: РГСУ, 2009. – №4 (67). (0,6 п.л., с. 77-81).

2. Пахарева Е.Н. Защита пользователей от распространения контента террористического характера в сети интернет: политологический аспект проблемы // Социальная политика и социология: междисциплинарный научно-практический журнал. – М.: РГСУ, 2010. – №2(56). (0,65 п.л., с. 80-94).

3. Пахарева Е.Н. Влияние кибертерроризма на молодежную среду: особенности и тенденции развития // Ученые записки Российского государственного социального университета. – М.: РГСУ, 2011. – №2 (90). (0,6 п.л., с. 51-56).

Публикации в других научных изданиях:

4. Авцинова Г.И., Пахарева Е.Н. Политическое противодействие кибертерроризму в международном сообществе и в Российской Федерации: управленческий аспект // Научные публикации кафедры политологии и социальной политики РГСУ. Выпуск №1. – М., РГСУ, 2008. – 226 с. (1,3 п.л., из них авторских 1 п.л., с. 25-44).

5. Пахарева Е.Н. Кибертерроризм в аспекте глобализации // Красновские чтения. Выпуск 2 / Отв.ред. Е.Н. Тарасов. – М.:АПКиППРО, 2008. – 246 с. (0.6 п.л., с. 108-117).

6. Пахарева Е.Н. Анализ угроз киберетрроризма и политика противодействия // Проблемы социального обновления России в исследованиях молодых ученых: Материалы выступлений на Аспирантских чтениях 18 апреля 2009 года/ под ред. Л.В. Прохоровой. – М.: АПКиППРО, 2009. – 428 с. (0,3 п.л., с. 71-76).

7. Пахарева Е.Н. Государственное регулирование сети Интернет в целях противодействия кибертерроризму // Аспирантский сборник №4 (37). М.: РГСУ, 2009. – 144 с. (0,8 п.л., с. 105-120).

8. Пахарева Е.Н. Угрозы кибертерроризма в современном информационном обществе // Инновационные подходы в исследованиях молодых ученых: Материалы выступлений на Аспирантских чтениях 20 апреля 2010 года/ под ред. А.В. Гапоненко. – М.: АПКиППРО, 2010. – 480 с. (0.3 п.л., с.99-105).

9. Пахарева Е.Н. Политика противодействия кибертерроризму как задача международной политики государства // Научные исследования кафедры политологии и социальной политики РГСУ. Сборник научных трудов. Выпуск 3. / Отв. ред. Г.И. Авцинова. М.:РГСУ, АПКиППРО, 2010. – 172 с. (0,75 п.л., с. 120-131).