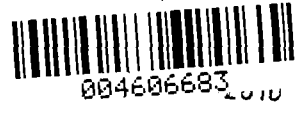
На правах рукописи

Кохтюлина Ирина Николаевна

МЕЖДУНАРОДНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ

Специальность 23.00.04 – политические проблемы международных отношений, глобального и регионального развития



Автореферат

диссертации на соискание ученой степени кандидата политических наук

Москва - 2010

Работа выполнена на кафедре национальных и федеративных отношений Федерального государственного образовательного учреждения высшего профессионального образования «Российская академия государственной службы при Президенте Российской Федерации»

Научный руководитель: доктор исторических наук, профессор
Дахин Владимир Никитович

Официальные оппоненты: доктор политических наук, профессор
Генчев Камен Генчев

кандидат политических наук
Портнягина Ирина Игоревна

Ведущая организация: **Дипломатическая академия МИД России**

Защита состоится 24 июня 2010 года в 12.00 часов на заседании Диссертационного совета Д 502.006.14 при РАГС по адресу: 119606, Москва, пр. Вернадского, д. 84, 1-й учебный корпус, ауд. 2200.

С диссертацией можно ознакомиться в научной библиотеке РАГС (1-й учебный корпус).

Автореферат разослан 24 мая 2010 года.

Ученый секретарь Диссертационного совета
доктор юридических наук, профессор

Л.Ф.Болтенкова

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность диссертационного исследования.

Завершается первое десятилетие XXI века. Оно по праву может войти в скрижали цивилизации как одно из самых драматичных. Наиболее емко сложившаяся ситуация оценена в Стратегии национальной безопасности Российской Федерации до 2020 года, утвержденной Президентом России Д.А.Медведевым 12 мая 2009 г.: «Возросла уязвимость всех членов международного сообщества перед лицом новых вызовов и угроз».[1]

В условиях феноменального развития информационно-коммуникационных технологий (ИКТ) проблема кибербезопасности, а также разработки и применения информационного оружия трансформируется из технологической в политическую. Так, по данным ЦРУ, его разработкой занято свыше 120 стран мира, в то время как разработкой оружия массового поражения – около 30. В силу этого ООН, ШОС, ОДКБ и иные международные организации в последнее время неоднократно принимали резолюции по обеспечению международной информационной безопасности (МИБ).

Актуальность исследуемой проблематики отмечена в Доктрине информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895)[2], Концепции внешней политики Российской Федерации (утверждена Президентом Российской Федерации 12 июля 2008 г. № Пр-1440)[3], в Стратегии развития информационного общества в Российской Федерации (утверждена Президентом Российской Федерации 7 февраля 2008 г. № Пр-212)[4], Концепции формирования в Российской Федерации электронного правительства до 2010 года (одобрена распоряжением Правительства

---

[1] Стратегия национальной безопасности Российской Федерации до 2020 года // «Собрание законодательства РФ», 18.05.2009, № 20, ст. 2444.

[2] Доктрина информационной безопасности Российской Федерации // «Российская газета», 28.09.2000, № 187.

[3] *Концепция внешней политики* РФ от 12.06.2008 г. http://www.kremlin.ru/text/decs/2008/07/204108.shtml

[4] Стратегия развития информационного общества в Российской Федерации // «Российская газета», 16.02.2008, № 34.

Российской Федерации от 6 мая 2008 г. № 632-р)[1], а также в Военной доктрине Российской Федерации (утверждена Указом Президента Российской Федерации 5 февраля 2010 г. № 146)[2]. В Послании Президента России Федеральному Собранию Российской Федерации (12 ноября 2009 г.) подчеркивается, что «в XXI веке главная ставка делается именно на развитие ИКТ, а одно из приоритетных направлений для России - развитие стратегических и информационных технологий»[3].

Рассматриваемая тема включена в перечень приоритетных проблем научных исследований в области обеспечения информационной безопасности Российской Федерации, утвержденный Советом Безопасности Российской Федерации 7 марта 2009 г. (п.40)[4].

Цель усилий России по обеспечению МИБ – не допустить очередного витка гонки вооружений на качественно новом уровне развития ИКТ, сохранить ресурсы в интересах развития, ограничить агрессивное использование этих технологий для силового разрешения межгосударственных противоречий.

В этом контексте в МИБ выделяют следующие три составляющие: военно-политическую, криминальную (киберпреступность) и террористическую (кибертерроризм).

Особую актуальность исследуемой проблеме придает тот факт, что информационно-коммуникационные технологии способны стать принципиально новым мощным средством разрушающего латентного воздействия на критически важные объекты государственного и военного управления, производственной и экономической сфер, социальной инфраструктуры, т.е. стать средством ведения геополитической борьбы.

Степень научной разработанности проблемы.

Работа базируется на современном исследовательском материале, монографиях, аналитических докладах, диссертационных исследованиях, научных статьях отечественных и зарубежных ученых, материалах научных конференций. Международные и политические аспекты изучаемой проблематики рассматриваются в работах таких авторов, как Д.С.Черешкин «Проблемы управления информационной безопасностью»

---

[1] Концепция формирования в Российской Федерации электронного правительства до 2010 года // «Собрание законодательства РФ», 19.05.2008, № 20, ст. 2372.

[2] Военная доктрина Российской Федерации // «Собрание законодательства РФ», 15.02.2010, № 7, ст. 724.

[3] http://www.kremlin.ru/transcripts/5979

[4] http://www.scfg.gov.ru/documents/93.html

(М., 2002 г.), В.Н.Дахин, С.А.Проскурин «Политические проблемы глобализации» (М., 2003 г.), А.И.Смирнов «Информационная глобализация и Россия: вызовы и возможности» (М., 2005 г.), А.А.Стрельцов «Правовое обеспечение информационной безопасности России: теоретические и методологические основы» (Минск, 2005 г.), А.В.Федоров «Информационная безопасность в мировом политическом процессе» (М., 2006 г.), А.В.Крутских «К политико-правовым основаниям глобальной информационной безопасности» (М., 2007), А.И.Буркин, А.В.Возженников, Н.В.Синеок «Национальная безопасность России в контексте современных политических процессов» (М., 2008), В.П.Шерстюк «Проблемы обеспечения международной информационной безопасности» (М., 2009 г.), изданиях «Международная безопасность России в условиях глобализации» под общ.ред. В.А.Михайлова, В.С.Буянова (М., 2007 г.), «Инновационные направления современных международных отношений» под ред.А.В.Крутских, А.В.Бирюкова (М., 2010 г.), сборнике статей «Национальная безопасность России в условиях трансформации международных отношений» (М., 2009), диссертационных исследованиях И.Л.Сафроновой «Политические проблемы обеспечения международной информационной безопасности» (М., 2006), Д.В.Маркарьяна «Информационно-коммуникационные технологии как фактор международных отношений: политические и правовые аспекты» (М., 2008), К.А.Кокунова «Вызовы и угрозы национальной безопасности России в условиях глобализации» (М., 2009). Экономическая компонента информационной безопасности в условиях становления глобального информационного общества затрагивается в работах И.А.Стрелец «Новая экономика и информационные технологии» (М., 2003 г.) и «Сетевая экономика» (М, 2006 г.).

Среди зарубежных авторов по исследуемой проблематике заслуживают внимания работы Д.Белла «The Coming of Postindustrial Society. A Venture in Social Forecasting». (N.Y.; 1973), М.Кастельса «Информационная эпоха: экономика, общество и культура» (М., 2000 г.), И.Масуды «The Information Society as Postindustrial Society» (Washington, 1983), М.Пората, М.Рубина «The Information Society: Development and Measurement» (Washington, 1978), А.Тоффлера «Creating of New Civilization: the Politics Of the Third Wave» (Atlanta, 1995).

Вместе с тем, приходится констатировать, что указанные исследования отстают от стремительного развития ИКТ и новых вызовов и

угроз в сфере информационной безопасности и особо ее международной составляющей. Автор предпринял попытку проанализировать международные аспекты информационной безопасности в условиях глобализации, в том числе раскрыть их актуальность для России с учетом зарубежного опыта.

Основная гипотеза исследования.

В последнее десятилетие объектом пристального внимания политологов стали внешнеполитические аспекты информационной безопасности. Информационно-коммуникационные технологии, став локомотивом процессов глобализации, одновременно породили принципиально новые вызовы и угрозы, соизмеримые с оружием массового поражения. В этих условиях для России, взявшей курс на модернизацию и вхождение в глобальное информационное общество, недопустима эрозия национальной безопасности в информационной сфере.

Объектом исследования являются международные аспекты информационной безопасности Российской Федерации в условиях глобализации.

Предмет исследования – новые явления и факторы, определяющие состояние и тенденции информационной безопасности России в международной сфере, а также риски, опасности и угрозы в данной области, в том числе в условиях глобальных кризисных явлений.

Цель исследования состоит в комплексной оценке состояния и тенденций международных аспектов информационной безопасности России в условиях глобализации, обосновании путей и механизмов ее обеспечения, выявлении специфических интересов, задач и возможностей Российской Федерации в данной области в новых геополитических условиях.

Задачи исследования направлены на достижение поставленной цели и состоят в следующем:

- выявить масштабы и основные тенденции развития информационно-коммуникационных технологий как локомотива глобализационных процессов в мире;
- раскрыть взаимосвязь национальной и информационной безопасности Российской Федерации в современных условиях;
- охарактеризовать внешнеполитические аспекты информационной безопасности в контексте Стратегии развития информационного общества

в России и Концепции формирования в Российской Федерации электронного правительства до 2010 года;

- проанализировать и систематизировать зарубежный опыт использования ИКТ для повышения эффективности информационной безопасности внешнеполитической деятельности на примере Соединенных Штатов Америки, Европейского Союза и Китая;

- определить актуальные задачи по эффективному обеспечению информационной безопасности в условиях инновационного развития России;

- исследовать приоритеты и перспективы обеспечения информационной безопасности Российской Федерации.

Хронологические рамки исследования - преимущественно последние два десятилетия.

Теоретическая основа исследования.

Проблемы информационной безопасности рассматриваются в рамках данной работы как особая междисциплинарная область знания. Теоретическую основу исследования составляют положения и выводы отечественных и зарубежных ученых, исследовавших доктринальные и концептуальные особенности международной информационной безопасности.

Методологическая основа исследования.

При подготовке диссертации автор опирался на труды ведущих российских и зарубежных ученых по изучаемой проблематике. Исследование выполнено с использованием основных методов политического анализа: системного, сравнительного, статистического, ситуационного, информационного и факторного.

Эмпирическая база исследования.

Многоаспектный формат вопросов, затронутых в диссертации, предопределил необходимость привлечения для анализа документов ООН, Международного союза электросвязи (МСЭ), ШОС, ОДКБ и других международных и региональных организаций, специальной литературы по проблемам, относящимся к информационной безопасности государства в условиях глобализации.

Информационную основу диссертации составляют официальные данные министерств и ведомств, документы международных институтов и общественных организаций, а также профессиональные издания, издаваемые в России и за рубежом. Политическая направленность

исследования потребовала привлечения соответствующих официальных документов, а также нормативных актов, принятых на национальном, региональном и многостороннем уровнях.

Основные положения, выносимые на защиту:

1. Автор полагает, что в современной политической науке не в полной мере отражены глобальные вызовы и угрозы, создаваемые информационной революцией. В этой связи предлагается рассматривать проблематику международной информационной безопасности в неразрывной триаде угроз: военно-политического, криминального и террористического характера.

2. Курс России на инновационное развитие значительно актуализировал проблематику обеспечения МИБ для национальных интересов, что нашло отражение в Стратегии национальной безопасности России до 2020 года в части информационной безопасности. С учетом того, что решение данной проблемы невозможно силами одного государства, Россия предпринимает значительные усилия по продвижению МИБ как в двустороннем формате международного сотрудничества, так и в формате ООН, «Группы восьми», ШОС, ОДКБ и др.

При этом автор полагает противодействовать использованию в качестве универсального договорного документа в сфере МИБ Конвенции Совета Европы о киберпреступности 2001 года в интересах подготовки соответствующего документа под эгидой ООН.

3. Опыт внедрения ИКТ на примере США, Европейского Союза и Китая, которые применяют различные модели электронного правительства (США – G2B, Евросоюз – G2C, Китай – G2B+G2C), демонстрирует ключевую роль обеспечения информационной безопасности.

4. Использование ситуационно-кризисных центров (СКЦ) как производной управленческой и информационной революций позволяет не только вести проблемный мониторинг вопросов внутренней и внешней политики, включая проблему МИБ, но и требует усиления защиты, поскольку в СКЦ концентрируется огромное количество оперативно значимой информации.

Основные научные результаты, полученные лично автором, и их научная новизна состоят в комплексном политологическом анализе состояния и тенденций международных аспектов информационной безопасности на современном этапе с раскрытием ее актуальности для

России и обоснованием путей и механизмов обеспечения информационной безопасности в условиях стремительного развития ИКТ и новых вызовов и угроз, порождаемых ими:

- уточнено соотношение информационной и других составляющих национальной безопасности России в условиях глобализации;

- определены новые риски, опасности и угрозы в контексте международной информационной безопасности в связи с бурным прогрессом ИКТ, в том числе для критически важных объектов;

- систематизирован зарубежный опыт использования ИКТ, информационных ресурсов для повышения уровня национальной безопасности на примере США, Европейского Союза и Китая;

- с учетом анализа передового зарубежного опыта сформулирован тезис о целесообразности продвижения системы распределенных ситуационно-кризисных центров с принятием дополнительных мер по обеспечению информационной безопасности.

Теоретическая значимость результатов исследования заключается прежде всего в систематизации доктринальных и концептуальных документов международного и внутрироссийского характера, посвященных проблематике информационной безопасности.

Практическая значимость результатов исследования состоит в том, что положения и выводы диссертации могут быть использованы в практической работе федеральных органов государственной власти России (Советом Федерации Федерального Собрания Российской Федерации, Государственной Думой Федерального Собрания Российской Федерации, Министерством иностранных дел Российской Федерации, Министерством коммуникаций и связи Российской Федерации, Министерством по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий Российской Федерации); при подготовке материалов для межведомственных ситуационных анализов, в т.ч. по вопросам международной информационной безопасности.

Материалы диссертации могут быть включены в учебный процесс в ВУЗах при чтении курсов «Национальная безопасность», «Информационно-коммуникационные технологии в государственном управлении».

Апробация исследования.

Диссертация подготовлена на кафедре национальных и федеративных отношений РАГС при Президенте Российской Федерации.

Результаты исследования были доложены автором на Всероссийской конференции «Безопасность информации и доступ к информации в кредитно-финансовой сфере» в рамках Национального форума информационной безопасности «ИНФОФОРУМ» 3 октября 2008 г. (доклад на тему: «Некоторые аспекты информационной безопасности на внешнеэкономическом треке»), а также нашли отражение в научных публикациях соискателя общим объемом около 7,2 п.л.

Структура работы состоит из введения, трех глав, заключения, списка использованной литературы и приложений.

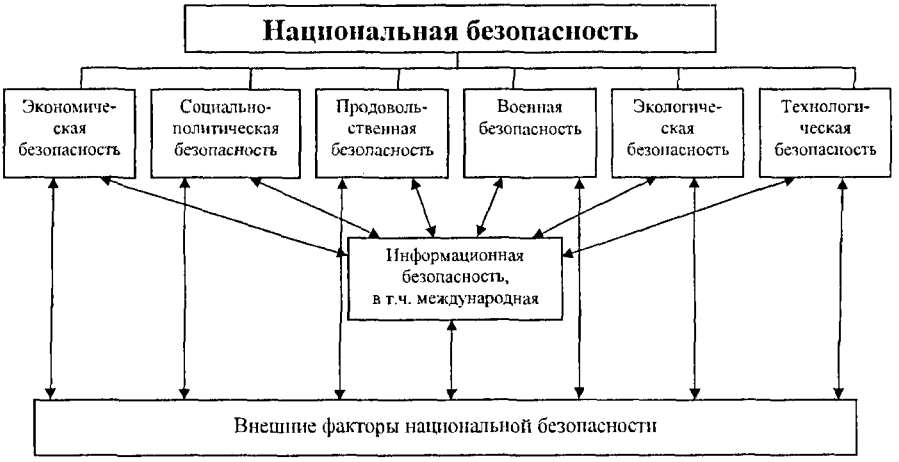
II. ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **Введении** обосновывается актуальность темы, характеризуется состояние ее научной разработанности, определены объект, предмет, цели и задачи исследования, хронологические рамки, формулируются положения, выносимые на защиту, раскрывается научная новизна, теоретическая и практическая значимость полученных результатов, содержатся сведения об их апробации.

В первой главе «Национальная безопасность России в условиях информационной глобализации» рассматривается влияние ИКТ на процессы глобализации, дается методологический анализ становления информационной составляющей национальной безопасности России, в том числе в контексте Стратегии развития информационного общества в России и Концепции формирования в Российской Федерации электронного правительства до 2010 года.

Подчеркивается, что в условиях глобализации значительно повышается роль внешней составляющей национальной безопасности, новых вызовов и угроз, к числу которых относятся риски, связанные со стремительным развитием ИКТ и их радикальным воздействием на все стороны общественной жизни, усилением значимости информационных ресурсов в политике, экономике, конкурентной борьбе. ИКТ становятся важнейшим фактором обеспечения стратегических интересов страны на международной арене. Отсюда – тесная взаимосвязь информационной и иных составляющих национальной безопасности России (схема 1).

Схема 1



В главе исследуется эволюция системы взглядов и подходов к обеспечению информационной составляющей национальной безопасности в Российской Федерации путем анализа основополагающих документов РФ (перечислены на стр. 3, 4 автореферата), фактов, а также трудов зарубежных и российских ученых по изучаемой проблематике

Автор соглашается с мнением ряда экспертов, называющих современный этап глобализации «информационной глобализацией», т.к. практически все действия, события и явления в мире становятся доступными в режиме реального времени.

В этих условиях в России политическим документом, позволяющим интегрально определять основные направления деятельности по формированию информационного общества, стала Стратегия развития информационного общества в России. Одновременно в ней подчеркнуто, что одна из основных целей государства в настоящее время – это противодействие угрозам использования потенциала ИКТ для нанесения ущерба национальным интересам России.

Проведенный автором анализ показал, что в реализации указанной Стратегии имеется ряд недостатков. Так, на заседаниях Совета при Президенте России по развитию информационного общества 12 февраля

2009 г. и 23 декабря 2009 г. подчеркивалось, что в России, несмотря на наличие интеллектуальных ресурсов и довольно быстрое распространение новых технологий и телекоммуникаций в последние годы, отставание от стран, лидирующих в этой сфере, только увеличивается. По рейтингу электронной готовности (e-readiness) в 2008-2009 гг. Россия занимала 59 место[1] (таблица 1).

Таблица 1

РЕЙТИНГ ЭЛЕКТРОННОЙ ГОТОВНОСТИ, 2009

Место, 2009	Место, 2008	Страна	Коэфф. эл.готовности, 2009	Коэфф. эл.готовности, 2008
1	5	Дания	8.87	8.83
2	3	Швеция	8.67	8.85
3	7	Нидерланды	8.64	8.74
4	11	Норвегия	8.62	8.60
5	1	США	8.60	8.95
6	4	Австралия	8.45	8.83
7	6	Сингапур	8.35	8.74
8	2	Гонконг	8.33	8.91
9	12	Канада	8.33	8.49
10	13	Финляндия	8.30	8.42

56	56	Китай	4.33	4.85
57	57	Египет	4.33	4.81
58	54	Индия	4.17	4.96
59	59	Российская Федерация	3.98	4.42
60	63	Эквадор	3.97	4.17
61	62	Нигерия	3.89	4.25

Источник: The Economist Intelligent Unit, 2009

[1] http://www-05.ibm.com/ie/pdf/E-readiness_rankings_2009.pdf

При этом органами власти крайне неэффективно используются ИКТ, фактически отсутствует «электронное правительство», межведомственный электронный документооборот с соответствующим обеспечением информационной безопасности.

Соискатель делает вывод, что интенсивное развитие ИКТ, являясь основой современного этапа процесса глобализации, становится движущей силой политических и экономических связей в мире с приданием принципиально нового качества международному информационному обмену.

Широкое внедрение ИКТ во все сферы общественной жизни усилило зависимость государства и общества от устойчивой работы информационных и телекоммуникационных систем, сохранности информационных ресурсов. При этом повышается уязвимость всех членов международного сообщества перед лицом новых рисков, опасностей и угроз в информационной сфере.

Вторая глава «Проблема международной информационной безопасности: внешнеполитическое измерение» содержит анализ основных трендов в проблематике МИБ в ООН, странах «Группы восьми», Международного союза электросвязи, ШОС, ОДКБ и других международных и региональных организациях, а также в России, в том числе в условиях глобального финансово-экономического кризиса.

В работе подчеркивается, что основная озабоченность мирового сообщества в сфере обеспечения МИБ связана с возможностью применения ИКТ в целях, не совместимых с задачами обеспечения международной стабильности и безопасности. В этом контексте обсуждение проблем противодействия угрозам применения информационного оружия для достижения политических целей посредством оказания «силового» давления на руководство противостоящих государств приобретает приоритетное значение.

Россия стала первым государством, поставившим на международном уровне вопрос о появлении принципиально новых – информационных – угроз национальной и международной безопасности в XXI веке, направив в 1998 г. соответствующее письмо в ООН. Важнейшей задачей в этом плане является ограничение угроз применения информационного оружия против критически важных объектов потенциального противника, равно как и враждебного использования ИКТ в качестве инструмента

межгосударственного противоборства, а также его применения в преступной и террористической деятельности.

Тема обеспечения МИБ с подачи России заняла прочное место в повестке дня целого ряда авторитетных международных форумов, включая ОБСЕ, ШОС, ОДКБ, Совет Европы, «Группу восьми», Международный союз электросвязи, Форум по управлению Интернетом, созданного под эгидой ООН.

В ходе работы 64-й сессии Генассамблеи ООН (2 декабря 2009 г.), как и в предыдущие годы, было обеспечено принятие предложенной Россией резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Таким образом, закреплена лидирующая роль России в рамках ооновского трека в решении проблемы МИБ на глобальном уровне.

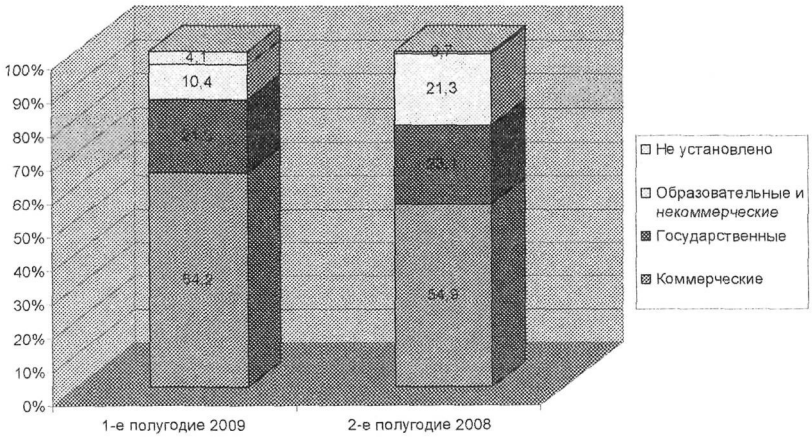
Принципиально важно, что в соответствии с резолюцией, принятой на 63-й сессии Генассамблеи ООН, под председательством России создана Группа правительственных экспертов ООН (ГПЭ) по МИБ, которая продолжит исследование угроз в сфере информационной безопасности. Основываясь на итогах работы ГПЭ, Генеральный секретарь ООН представит 65-й сессии Генассамблеи ООН (сентябрь 2010 г.) доклад о результатах данного исследования.

Очевидно, что российское председательство в ГПЭ будет реально способствовать продвижению на международной арене инициативной позиции России, направленной на формирование всеобъемлющей системы МИБ.

В диссертации отмечается, что глобальный финансово-экономический кризис потребовал принятия комплексных скоординированных и устойчивых мер по задействованию политических и экономических инструментов по его преодолению, в том числе на треке киберпреступлений (схема 2).

Схема 2

Распределение источников утечек по видам организаций[1]



Источник: InfoWatch

В этих условиях угрозы информационной и экономической безопасности становятся все более сложными и приобретают глобальный характер. Информационная безопасность, давно вышедшая за рамки борьбы с известными киберпреступлениями, определенными Интерполом (хакинг[2], крекинг[3] и т.д.), а также вирусами и шпионскими программами, часто включает в себя юридические, идентификационные и геополитические факторы.

Так, международное право значительно отстало от развития ИКТ, для которых понятия «граница» и «территория государства» потеряли смысл, ибо и «граница», и «территория государства» стали легко проницаемыми и транспарентными для современных информационных технологий, игнорируя действующие международно-правовые дефиниции их статуса.

---

[1] http://www.cnews.ru/reviews/index.shtml?2009/08/25/359105

[2] Хакинг – взлом ИКТ-системы путем обхода или отключения мер по обеспечению информационной безопасности.

[3] Крекинг – криминальный хакинг (киберпреступление).

Базируясь на проведенном анализе, автор делает вывод о том, что даже в условиях кризиса государственные и бизнес структуры сохранили расходы на информационную безопасность в среднем на докризисном уровне при общем сокращении бюджетов. В силу этого решение проблемы МИБ диктует всему мировому сообществу принятие дополнительных и скоординированных усилий.

В третьей главе «Приоритеты и перспективы обеспечения информационной безопасности в целях повышения конкурентоспособности Российской Федерации» критически проанализирован зарубежный опыт предотвращения угроз, связанных с использованием ИКТ, на примере США, Европейского Союза и Китая, исследована проблематика построения и дальнейшей реализации инновационной модели экономического развития России с учетом требований информационной безопасности.

В работе отмечается, что в США, Европейском Союзе и Китае уже в конце XX века осознали невозможность решения проблем XXI века без опоры на цифровые технологии. При этом на повестке дня деятельности правительств рассматриваемых субъектов международных отношений, базовым является вопрос обеспечения информационной безопасности, включая международное сотрудничество в данной сфере. В диссертации данный постулат подтверждается тем, что в основополагающих документах, касающихся национальной безопасности каждой из стран, единственным путем обеспечения кибербезопасности определено принятие скоординированных превентивных мер.

Для России использование ИКТ – неотъемлемая составляющая инновационной модели экономического развития. При этом, как подчеркнуто в послании Д.А.Медведева Федеральному Собранию Российской Федерации (12 ноября 2009 г.), «выбор приоритетов модернизации экономики и технологического развития главным образом связан с обеспечением безопасности»[1].

Соглашаясь с выводом ряда экспертов о том, что в России одна из основных задач государства - противодействие угрозам использования потенциала ИКТ для нанесения ущерба национальным интересам России, автор одновременно полагает, что особой защиты требуют ситуационно-кризисные центры (СКЦ), так как в них обрабатывается и концентрируется

[1] http://www.kremlin.ru/transcripts/5979

критически важная информация, в том числе по международному сотрудничеству.

СКЦ получили широкое распространение за рубежом (МИД Германии, Франции, Италии, оперативный центр Государственного департамента США и др.), поскольку СКЦ, интегрирующие в себе достижения информационной и управленческой революций позволяют принципиально по-новому, инновационно отслеживать, анализировать, прогнозировать кризисные явления, а также оперативно реагировать на них.

В России в соответствии со Стратегией национальной безопасности России до 2020 года (п.107) ведется работа по организации системы распределенных ситуационных центров высших органов государственной власти. Высший уровень - это ситуационный центр Президента Российской Федерации, который, наряду с аналогичными комплексами президента США и правительства Германии, является одним из наиболее технически совершенных в мире. Функционируют ситуационные центры Администрации Президента Российской Федерации и Правительства Российской Федерации. На втором уровне находятся ситуационные центры полномочных представителей Президента Российской Федерации в федеральных округах, руководителей министерств (например, Национальный центр управления в кризисных ситуациях МЧС России), агентств (Росатом) и служб. На третьем уровне - ситуационные центры глав субъектов Российской Федерации и муниципальных образований.

При этом п.108 вышеуказанной Стратегии нацеливает на обеспечение информационной безопасности вышеуказанной системы ситуационных центров.

Диссертант исследует режимы работы СКЦ (проблемного мониторинга, кризисного реагирования, чрезвычайной ситуации), а также принципы их построения (локальный и распределенный), в том числе с использованием системы защищенной видеоконференцсвязи. Отмечается, что объектом ситуационного анализа в СКЦ являются самые разнообразные актуальные аспекты внутренней и внешней политики, включая проблематику международной безопасности, в том числе и вопросы МИБ.

Автор резюмирует, что СКЦ являются приоритетным и перспективным инструментарием как в целях повышения конкурентоспособности России на международном треке, так и

продвижения концептуальных положений международной информационной безопасности. Одновременно СКЦ сами нуждаются в повышенном уровне защиты, поскольку в них концентрируется чувствительная информация.

В **Заключении** сформулированы основные выводы и рекомендации, полученные по итогам проведенного исследования.

Во-первых, информационная революция наряду с очевидными благами для цивилизации создает для нее вызовы и угрозы во внешнеполитической сфере принципиально нового характера. Проведенный анализ трендов и перспектив межгосударственного сотрудничества, в том числе в формате ООН и других международных организаций по обеспечению МИБ подтверждает вышеуказанный вывод. Системное изучение проблематики МИБ показало, что способы и особенности использования ИКТ, включая латентные, во враждебных и неправомерных целях, имеют неразрывную триаду угроз информационной безопасности военно-политического, криминального и террористического характера. При этом военно-политическая составляющая играет приоритетную роль, в том числе и потому, что включает в себя информационно-психологическую безопасность.

Во-вторых, курс России на модернизацию экономики и перевод ее на инновационное развитие значительно актуализировал проблематику обеспечения МИБ для национальных интересов. Реализация Стратегии национальной безопасности России до 2020 года в части информационной составляющей способствует усилению координации действий федеральных органов государственной власти, в том числе по продвижению соответствующей резолюции ООН по МИБ, принятой 2 декабря 2009 г.

В-третьих, в качестве рекомендаций по подходам России в области формирования системы МИБ автор предлагает следующие:

- придание проблематике МИБ политической окраски, внесение данного вопроса в формат международных переговоров, имеющих непосредственное отношение к обеспечению международной и национальной безопасности и стабильности;

- проведение российского курса в сфере МИБ в ООН с акцентом на работу в 2010 г. Группы правительственных экспертов (ГПЭ) ООН по МИБ и целенаправленной работы со странами из числа представленных в ГПЭ ООН по МИБ – членами ШОС (Китай, Казахстан), БРИК (Бразилия,

Индия), Евросоюза (Франция, Германия, Италия), а также США, Канадой, Японией, Израилем, ЮАР;

- противодействие использованию в качестве универсального договорного документа в сфере МИБ Конвенции Совета Европы о киберпреступности 2001 года с подготовкой соответствующего документа под эгидой ООН;

- продвижение на международной арене открытого к присоединению Соглашения между правительствами государств-членов ШОС о сотрудничестве в области обеспечения МИБ от 16 июня 2009 г.;

- активизация работы государств-членов ОДКБ по формированию системы информационной безопасности, а также закрепление на международном уровне терминологии по проблематике МИБ, применяемой в России, а также согласованной в ШОС.

В-четвертых, проведенный анализ зарубежного опыта использования ИКТ на примере США, Европейского Союза и Китая показал, что основной целью этих государств является достижение лидирующих позиций в мире. Используя различные модели электронного правительства (США – G2B, Евросоюз – G2C, Китай – G2B+G2C), их правительства считают вопрос обеспечения информационной безопасности одним из ключевых. Так, в США в 2009 г. принят доктринальный документ Cybersecurity 2009.

В-пятых, анализ феномена резко расширяющегося внедрения ситуационно-кризисных центров в ведущих странах мира показал, что СКЦ способны стать одним из эффективных инструментариев повышения конкурентоспособности России, путем исследования проблематики внутренней и внешней политики, в том числе мониторинга и продвижения международных аспектов информационной безопасности.

III. Основные положения диссертационного исследования отражены в следующих публикациях:

I. Статья в издании, рекомендованном ВАК Министерства образования и науки РФ

1. Кохтюлина И.Н. Внешнеэкономические аспекты информационной безопасности: современные методы анализа // «Международная экономика». – 2009. – № 11. 0,5 п.л.

II. Публикации в других изданиях

1. Кохтюлина И.Н. Информационная составляющая внешнеэкономической безопасности Российской Федерации. – М.: Полпред, 2008. 6,4 п.л.
2. Кохтюлина И.Н. Некоторые аспекты информационной безопасности на внешнеэкономическом треке // «Бизнес и безопасность в России». – 2009. – № 52. 0,3 п.л.

Общий объем публикаций автора по теме исследования - 7,2 п.л.

Автореферат диссертации на соискание ученой степени кандидата политических наук

Кохтюлина Ирина Николаевна

Тема диссертационного исследования:

Международные аспекты информационной безопасности России в условиях глобализации

Научный руководитель:
доктор исторических наук, профессор
Дахин Владимир Никитович

Изготовление оригинал-макета
Кохтюлина Ирина Николаевна

Подписано в печать 21. 05. 2010 г. Тираж 80 экз.

Усл. п.л 1,1.

Федеральное государственное образовательное учреждение высшего профессионального образования «Российская академия государственной службы при Президенте Российской Федерации»

Отпечатано ОПМТ РАГС. Заказ 217.

119606, Москва, пр-т Вернадского, 84.