На правах рукописи

Сафронова Ирина Леонидовна

Политические проблемы обеспечения международной информационной безопасности

Специальность 23.00.04 – политические проблемы международных отношений и глобального развития

Автореферат диссертации на соискание ученой степени кандидата политических наук

Москва, 2006

Работа выполнена на кафедре мировых политических процессов Московского государственного института международных отношений (Университет) МИД России

Научный руководитель: доктор исторических наук,
профессор Крутских Андрей Владимирович

Официальные оппоненты: доктор технических наук,
доктор юридических наук
Стрельцов Анатолий Александрович

кандидат политических наук,
Мешкова Татьяна Анатольевна

Ведущая организация: Московский государственный университет имени М.В. Ломоносова, Социологический факультет, кафедра социологии международных отношений.

Защита состоится «21» сентября 2006 года в 10.00 на заседании Диссертационного совета Д.209.002.02 Московского государственного института международных отношений (Университет) МИД России по адресу: 119454, г. Москва, проспект Вернадского, д. 76.

С диссертацией можно ознакомиться в научной библиотеке МГИМО (У) МИД России по адресу: 119454, г. Москва, проспект Вернадского, д. 76.

Автореферат разослан: «20» июля 2006 года.

УЧЕНЫЙ СЕКРЕТАРЬ
ДИССЕРТАЦИОННОГО СОВЕТА

кандидат философских наук
Чанышев Александр Арсеньевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность исследования. В последние десятилетия достижения науки и технологий как никогда прежде начали определять динамику экономического роста, уровень благосостояния населения, конкурентоспособность государств в мировом сообществе, степень обеспечения их национальной безопасности и интеграции в мировую экономику.

Научно-техническая революция самым значительным образом затронула информационно-телекоммуникационную сферу, вызвав стремительное развитие и широкое использование информационно-коммуникационных технологий (ИКТ). Произошел переход от индустриального общества к постиндустриальному, характеризующемуся ростом предоставления и потребления услуг, в том числе информационно-коммуникационных, а также все более возрастающей ролью информационной сферы и информации[1].

ИКТ не только трансформировали принципы и формы сбора, обработки и передачи информации, но также начали оказывать мощнейшее воздействие на политический, военно-стратегический, экономический, социальный и культурный аспекты жизни государства и общества, становясь одним из основных факторов обеспечения устойчивого развития.

Информатизация вызвала к жизни образование межгосударственных альянсов – своего рода политических союзов, в основе которых лежит общность информационно-коммуникационных интересов. Стержнем деятельности таких объединений становится обеспечение широкого и недискриминационного доступа к ИКТ, проведение единой инфокоммуникационной политики, стремление к достижению максимальной конкурентоспособности, выходу на лидирующие позиции в мире. Такие альянсы могут возникать вокруг отдельных национальных инфокоммуникационных систем, региональных или международных телекоммуникационных проектов и организаций.

---

[1] В диссертационной работе под термином «информация» понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Развитие национальных, региональных и международных информационных инфраструктур, в том числе Интернет, стало важным фактором глобализации политических, экономических, социально-культурных и научно-образовательных процессов, международных отношений в целом. Это ознаменовало собой начало складывания глобального информационного общества (ГИО) – общества, скрепленного информационными технологиями и основывающегося на них, стремящегося к максимально широкому использованию всеми странами преимуществ информатизации посредством равноправного, эффективного и безопасного доступа к информации, информационно-коммуникационным технологиям и средствам.

Формирование ГИО оказало значительное влияние на всю систему современных международных отношений: были созданы условия для политического и экономического развития отдельных стран, их интенсивного включения в мировые интеграционные процессы, в формирующееся общее информационное пространство; открылись широчайшие позитивные возможности для расширения взаимодействия на общее благо всех государств, увеличения созидательного потенциала человечества и дополнительных сдвигов к лучшему в распространении информации в мире.

Процессы глобальной информатизации способствовали, через расширение круга субъектов информационного взаимодействия, увеличению числа акторов международных отношений, а также повышению активности и эффективности их участия в политических процессах. ИКТ, проникая во все сферы жизнедеятельности общества, обеспечили доступ граждан к самой различной информации, в том числе к государственным информационным ресурсам, позволили осуществлять контроль за деятельностью органов государственной власти, за состоянием экономики, экологии и других значимых сфер общественной жизни, развивать диалог между властными и гражданскими структурами.

Количество ИКТ, их технический уровень и доступность уже сегодня определяют уровень развития страны, ее статус, место, роль и геополитический потенциал в мировом сообществе и, бесспорно, станут решающими показателями этого статуса в самое ближайшее время. Сегодня правомерно утверждать:

чем большими возможностями в информационной сфере обладает государство, тем вероятнее при прочих равных условиях оно может добиться стратегических геополитических преимуществ и экономического процветания. В политической сфере все большее значение приобретают не силовые, а информационные факторы.

Вместе с тем высокая сложность и одновременно уязвимость всех систем, на которых базируются национальные, региональные и мировое информационные пространства, а также фундаментальная зависимость от их стабильного функционирования практически всех инфраструктур государств, в том числе критических, приводят к возникновению принципиально новых угроз. Эти угрозы связаны, прежде всего, с потенциальной возможностью использования ИКТ в целях, несовместимых с задачами поддержания международной безопасности, соблюдения принципов отказа от применения силы, невмешательства во внутренние дела государств, уважения прав и свобод человека.

Особые опасения в этом плане вызывают разработка, применение и распространение информационного оружия, в результате которых становятся возможны информационные войны, способные вызвать мировые катастрофы, разрушительные последствия которых могут быть сопоставимы с последствиями применения оружия массового уничтожения.

Информационное оружие использовалось во всех военных конфликтах в течение последних 10-15 лет: в Панаме (1989 год), на Гаити (1994 год), во время операции «Буря в пустыне», в Югославии (1999 год), Афганистане (2002 год) и Ираке (с 2003 года)[2].

Оно стало важной частью вооружения сил общего назначения США и их союзников. Новые информационные и телекоммуникационные технологии активно применяются спецслужбами. Имеются данные о том, что работы по развитию потенциала информационного противоборства проводятся более чем в 120 странах мира (разработки в области ядерного оружия ведут не более 20 стран)[3].

---

[2] Sweetman B. High Tech and Low Cunning / B. Sweetman // Jane's International Defense Review. – 2003, I March. – P. 79-83.

[3] Крутских А.В. Война или мир: международные аспекты информационной безопасности / А.В.Крутских // Политика. – 2001. – № 45. – С. 11.

Происходит трансформация всей военной информационной архитектуры: наблюдается «информатизация» традиционных вооруженных сил и «интеллектуализация» вооружений. Активно развивается концепция сетецентрического ведения военных действий, подразумевающая достижение превосходства над врагом путем эффективной организации сбора, обработки и использования информации. Информация при этом становится центральным элементом планирования военных операций и управления ими.

Операции по достижению превосходства в информационном пространстве зачастую ведутся в небоевой обстановке и проводятся за месяцы или даже годы до начала военной операции. Военное по своей сути воздействие начинается без объявления войны, в мирное время. Информационные операции превращаются, таким образом, из вида боевых действий в самостоятельное мероприятие.

Применение инфооружия может не вызывать разрушения объектов физической инфраструктуры и гибели людей. Жертва подчас может не осознавать, что находится под информационным воздействием. Тем не менее, в результате таких действий происходит ослабление противника, и война может быть выиграна до ее начала. Можно прогнозировать, что в будущем роль информационного противоборства при проведении военных операций будет возрастать.

Использование информационного оружия не требует больших финансовых затрат, что делает информационную войну экономичным и потому весьма опасным средством вооруженной борьбы. Инфооружие не знает географических расстояний, оно подрывает традиционное понятие государственных границ, делая их технологически проницаемыми. Его применение носит обезличенный характер и позволяет замаскировать разрушительную по своим масштабам информационную операцию, проведенную государством, под киберпреступление, источник которого так и останется неизвестным, или акт кибертерроризма, реализованный международными террористами, не имеющими государственной принадлежности.

Активизируется киберпреступность, которая в настоящее время рассматривается многими экспертами как стремительно нарастающая угроза безопасности как для отдельных государств, так и для мирового сообщества в целом. Несмотря на усилия правоохранительных органов и спецслужб,

направленные на борьбу с киберпреступностью и кибертерроризмом, число преступных актов с использованием ИКТ не уменьшается, а, напротив, постоянно увеличивается, возрастает их общественная опасность.

Интернет стал той сферой, где преступность растет самыми быстрыми темпами на планете. Каждый год в мире фиксируются сотни тысяч попыток несанкционированного вмешательства в государственные, военные, банковские, корпоративные компьютерные системы, компьютеры отдельных пользователей. Киберпреступность становится все более глобальной, масштабной по техническим, экономическим и возможным политическим последствиям. Участились хакерские проникновения в сети государственных ведомств, в том числе оборонных.

Ежегодные финансовые потери от незаконной деятельности с использованием новых Интернет-технологий превышают 80 млрд. долл. США. Причем целью киберпреступников зачастую являются не ресурсы Интернет и электронные платежные системы, как это нередко представляется в печати, а средства, связанные с управлением государством, экономикой.

Меняется облик терроризма, о чем наглядно свидетельствует появление информационного терроризма. Анализ ставших известными кибератак показывает, что ИКТ уже освоены международными террористическими и экстремистскими организациями (ХАМАС, Аль-Каида).

ИКТ предоставляют террористам возможность скрытно, планомерно и эффективно воздействовать на индивидуальное и массовое сознание, общественное мнение, процессы принятия решений; распространять информацию для вербовки в свои ряды новых членов, пропаганды собственных идей; осуществлять сбор денежных средств для финансирования своей деятельности; проводить дезинформацию; вызывать панику, а также непосредственно совершать террористические акты.

По оценкам экспертов, террористы уже сегодня способны использовать такие средства электронного воздействия, как, например, высокомощное микроволновое оружие, применение которого будет наиболее эффективным против критических информационных инфраструктур[4].

---

[4] Sirak M. U.S. vulnerable to EMP Attack // Jane's Defense Weekly. – 2004. – 26 July // http://www.janes.com/defence/news/jdw/jdw040726_1_n.shtml.

Нельзя не отметить, что под эгидой борьбы с международным терроризмом отдельными странами осуществляется систематическое вмешательство во внутренние дела других государств, подрывающее суверенитет последних.

Разработка, производство, использование и распространение информационного оружия, рост киберпреступности и информационного терроризма представляют серьезную угрозу для международной стабильности и безопасности. Они стали важным фактором, непосредственно влияющим на формирование международных отношений, и приобретают особую остроту в связи со значительным отставанием международного права от стремительно развивающихся информационных отношений в обществе, недостаточностью существующих международно-правовых норм, регулирующих такие отношения, и многосторонних механизмов обеспечения международной информационной безопасности.

Степень разработанности проблемы. Внимание ученых-исследователей к проблемам информатизации, построения информационного общества, а также информационной безопасности в последнее время значительно возросло.

Общие политические последствия информатизации исследуют такие российские ученые, как Р.Ф. Абдеев, А.Т. Багиров, Д.Г. Балуев, О.Н. Вершинская, В.Л. Иноземцев, М.М. Лебедева, И.С. Мелюхин, С.А. Модестов, Д.Н. Песков, А.И. Смирнов, Д.М. Фельдман, П.А. Цыганков[5].

---

[5] Среди наиболее значимых работ можно выделить следующие: Абдеев Р.Ф. Философия информационной цивилизации / Р.Ф. Абдеев. – М.: ВЛАДОС, 1994; Багиров А.Т. Интернет в международных отношениях / А.Т. Багиров // Международная жизнь. – 2000. – № 8-9; Балуев Д.Г. Новые информационные технологии и современные международные отношения / Д.Г. Балуев. – Нижний Новгород: Нижегородский государственный университет, 1998. – 47 с.; Новая постиндустриальная волна на Западе: Антология / Под ред. В.Л. Иноземцева. – М.:Academia, 1999; Иноземцев В. Парадоксы постиндустриальной экономики (инвестиции, производительность и хозяйственный рост в 90-е годы) / В. Иноземцев // Мировая экономика и международные отношения. – 2000. – № 3; Лебедева М.М. Мировая политика и международные отношения на пороге нового тысячелетия / Под ред. М.М. Лебедевой. – М.: Московский общественный научный фонд, 2000; Лебедева М.М. Современные технологии и политическое развитие мира / М.М. Лебедева // Международная жизнь. – 2001. – № 2; Модестов С.А. Информационное противоборство как фактор геополитической конкуренции / С.А. Модестов. – М.: Московский общественный научный фонд, издательский центр научных и учебных программ, 1994. – 64 с.; Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности / А.И. Смирнов. – М.: Парад, 2005. – 392 с.; Фельдман Д.М. Информация и национальная безопасность России / Д.М. Фельдман // Власть. – 2001. – № 9. – С. 32-36.

Среди зарубежных авторов, изучающих данную проблематику, – О. Винкель, А. Гриффинс, М. Кастельс, Й. Ней, Р. Кеохане, Дж. Розенау, Ф. Фукуяма, Ф. Харви, М. Эган[6].

М.М. Лебедева отмечает, что в международных отношениях второй половины XX века все значимее становилась информационная компонента. При этом развитие трансграничных по своему характеру ИКТ рассматривается как один из важных факторов глобализации.

П.А. Цыганков утверждает, что в современных международных отношениях приоритетным национальным интересом становится обладание передовыми технологиями, обеспечивающими совместимость с самыми современными средствами информации и связи. Что касается военного фактора и связанных с ним стратегий, то они уже не занимают первого места в иерархии национальных интересов. Он подчеркивает, что выживание государства-нации сегодня зависит уже не столько от способности противостоять традиционным военным угрозам (хотя и их еще рано сбрасывать со счетов), сколько от возможности находить адекватные ответы на новые вызовы безопасности технологического и информационного характера[7].

Диссертационное исследование опирается на проводимый в большинстве упомянутых работ тезис о важнейшем значении информационных факторов в современной мировой политике и развивает его.

Механизмы трансформации роли государства и власти, в частности внешней политики и политики в области безопасности, в условиях глобальной

---

[6] Основные работы: Кастельс М. Информационная эра: экономика, общество и культура / М. Кастельс; Пер. с англ. под науч. ред. О.И. Шкаратана. – М.: ГУ-ВШЭ, 2000. – 608 с.; Кеохане Р.О. Информационная революция. Государство и власть в эпоху глобальной информации / Р.О. Кеохане, Й.С. Ней // Международная политика. – 2000. – № 10; Розенау Дж.Н. Новые измерения безопасности: взаимодействие глобальных и локальных динамик / Дж.Н. Розенау // http://www.auditorium.ru/books/723/17.htm; Фукуяма Ф. Великий разрыв / Ф. Фукуяма. – М.: АСТ, 2003. – 474 с.; Fukuyama F. The promise and challenge of emerging technologies / F. Fukuyama // http://www.rand.org/publications/MR/MR1139/MR1139.chap2.pdf; Egan M. The executive guide to information security: threats, challenges, and solutions / M. Egan. – Indianapolis, 2004; Harvey F.P. Foreign and security policy in the information age / F.P. Harvey, A.L. Griffinth. – Halifax: Centre for Foreign Policy Studies, 1999; Winkel O. The democratic potentials of interactive information technologies under discussion-problems, viewpoints, and perspectives / O. Winkel // International Journal of Communications Law and Policy. – 2000/2001. – № 6.

[7] Цыганков П.А. Теория международных отношений / П.А. Цыганков. – М.: Гардарика, 2005. – 590 с.

информационной революции, рассматривают Ю.Б. Кашлев[8], А. Гриффинс, Р. Кеохане, Й. Ней и Ф. Харви. На вопросах информационной политики Российской Федерации, в том числе роли государства в формировании информационного общества в России, подробно останавливаются И.Н. Курносов[9] и А.И. Смирнов[10].

Проблемы, связанные с уяснением содержания национальных интересов в информационной области, угроз этим интересам и проявлений таких угроз, а также деятельности по реализации национальных интересов и противодействию соответствующим угрозам, прорабатываются, в частности, В.А. Баришполец, А.В. Возжениковым, В.Н. Лопатиным, В.Л. Маниловым, А.А. Прохожевым, А.А. Стрельцовым[11].

В своей работе автор использует предложенную А.А. Стрельцовым структуру понятия «информационная безопасность», которое включает в себя такие элементы, как «объекты информационной безопасности», «угрозы объектам информационной безопасности» и «обеспечение информационной безопасности»[12], включив в эту модель дополнительную структурную единицу – «субъекты информационной безопасности» (преступные организации и отдельные преступники, в том числе хакеры; террористические группы, группировки и отдельные террористы; государства).

Интенсифицируются исследования проблем информационной безопасности в контексте политологии. В рамках этой дисциплины С.В. Коротков, А.В. Крутских,

---

[8] Кашлев Ю.Б. На передовом рубеже глобализация. Международное информационное общество и вызовы дипломату XXI века / Ю.Б. Кашлев // Дипкурьер НГ. – 2000. – 28 декабря // http://www.world.ng.ru/dipcorpus/2000-12-28/6_globalisation.html.

[9] Курносов И.Н. Роль государства в формировании информационного общества в России / И.Н. Курносов // Вестник РФФИ. 1999. – сентябрь. – № 3(17).

[10] Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности / А.И. Смирнов. – М.: Парад, 2005. – 392 с.

[11] Основные работы: Основы национальной безопасности России / М.И. Абдурахманов, В.А. Баришполец, В.Л. Манилов, В.С. Пирумов. – М.: Друза, 1998. – 327 с.; Абдурахманов М.И. Национальная безопасность России / М.И. Абдурахманов, В.А. Баришполец, В.Л. Манилов. – М.: ВЦ РАН, РАЕН, 2000 – 389 с.; Возженников А.В. Парадигма национальной безопасности реформирующейся России / А.В. Возженников. – М.: ЭДАС ПАК, 2000; Возженников А.В. Национальная безопасность России / А.В. Возженников. – М.: РАГС, 2002. – 424 с.; Лопатин В.Н. Информационная безопасность России: человек, общество, государство / В.Н. Лопатин. – СПб.: Университет МВД России, 2000; Манилов В.Л. Безопасность в эпоху партнерства / В.Л. Манилов. – М.: Терра, 1999. – 368 с.; Прохожев А.А. Национальная безопасность: основы теории, сущность, проблемы / А.А. Прохожев. – М.: РАГС, 1997; Стрельцов А.А. Обеспечение информационной безопасности России / А.А. Стрельцов. – М.: МЦНМО, 2002. – 296 с.

[12] Стрельцов А.А. Обеспечение информационной безопасности России / А.А. Стрельцов. – М.: МЦНМО, 2002. – С. 57.

Г.С. Смолян, В.Н. Цыгичко, Д.С. Черешкин[13] рассматривают вопросы влияния угроз в информационной сфере на систему международных отношений, в том числе через призму геополитики. На передний план в их исследованиях выходит военно-политическая составляющая информационной безопасности. Так, А.В. Крутских отмечает: «прогресс в информационных технологиях, так же как ранее в ядерных, чреват новым витком гонки вооружений, который вновь может отвлечь огромные ресурсы человечества от целей мирного созидания»[14].

В диссертационном исследовании проведено углубленное, комплексное исследование угроз информационной безопасности военно-политического, террористического и преступного характера, выделяемых упомянутыми авторами, описаны их недостаточно изученные проявления, проанализированы их последствия и выявлены связи, которые могут существовать между этими угрозами.

Вопросы информационных войн исследуются такими отечественными авторами, как С.Н. Гриняев, В.А. Лисичкин, В. Малышев, В.К. Потехин, Г.Г. Почепцов, С.П. Расторгуев, А.В. Федоров, И. Шаравов[15]. В их работах рассматривается влияние информационного фактора на оборонную и военную сферы государств, тактику и стратегию ведения современных войн.

---

[13] Информационное оружие – новый вызов международной безопасности / В.Н. Цыгичко, Д.С. Вотрин, А.В. Крутских, Г.Л. Смолян, Д.С. Черешкин. – М.: Институт системного анализа РАН, 2000. – с. 52; Информационно-психологическая безопасность (определение и анализ предметной области) / Г.Л. Смолян, Г.М. Зараковский, В.М. Розин, А.Е. Войскунский. – М.: Институт системного анализа РАН, 1997. – 52 с; Информационные вызовы национальной и международной безопасности / И.Ю. Алексеева и др.; Под общ. ред. А.В. Федорова, В.Н. Цыгичко. – М.: ПИР-Центр, 2001. – 328 с.

[14] Крутских А.В. Война или мир: международные аспекты информационной безопасности // Политика. – 2001. – № 45. – С. 11.

[15] Основные работы: Гриняев С.Н. Интеллектуальное противодействие информационному оружию / С.Н. Гриняев. – М.: Синтег, 1999; Гриняев С.Н. Поле битвы – киберпространство / С.Н. Гриняев. – Минск: Харвест, 2004 – 448 с.; Информационные вызовы национальной и международной безопасности / И.Ю. Алексеева и др.; Под общ. ред. А.В. Федорова, В.Н. Цыгичко. – М.: ПИР-Центр, 2001. – 328 с.; Лисичкин В.А. Третья мировая (информационно-психологическая) война / В.А. Лисичкин, Л.А. Шелепин. – М.: Институт социально-политических исследований АСН, 2000. – 304 с.; Малышев В. Использование возможностей средств массовой информации в локальных вооруженных конфликтах / В. Малышев // http://www.cryptography.ru/db/msg.html?mid=1169389; Потехин В.К. Национальная безопасность: информационная компонента в современных войнах / В.К. Потехин // http://isn.rsuh.ru/cpis/win/confer/98_04/potekh.htm; Почепцов Г.Г. Информационные войны / Г.Г. Почепцов. – М.: Рефилл-бук, 2000; Расторгуев С.П. Философия информационной войны / С.П. Расторгуев. – М.: Вузовская книга, 2001. – 468 с.; Шаравов И. К вопросу об информационной войне и информационном оружии / И. Шаравов // http://ww-4.narod.ru/warfare/page0004.htm.

В диссертационной работе была использована предложенная А.В. Федоровым и В.Н. Цыгичко подробная классификация информационного оружия[16].

Аспекты информационной безопасности, связанные с содержательной стороной информации, изучаются Г.В. Грачевым, Ю.А. Ермаковым, В.Е. Лепским, В.А. Лисичкиным, Е. Месснером, И.К. Мельником, И.Н. Панариным, Г.Г. Почепцовым, А.А. Тепловым, Л.А. Шелепиным[17].

В диссертационной работе учтены информационно-психологические аспекты информационной безопасности, включая манипулирование личностью, воздействие на индивидуальное, групповое и массовое сознание, акцент на которые делается в работах этих исследователей.

Значительные результаты были достигнуты в правовом осмыслении процессов информатизации. Работы Ю.М. Батурина, В.В. Крылова, А.В. Черных, Н.Г. Шурухнова[18] заложили основы компьютерной криминалистики. Активно прорабатывают эту проблематику В. Номоконов, В. Сабадаш, Т. Тропина[19].

---

[16] Информационные вызовы национальной и международной безопасности / И.Ю. Алексеева и др.; Под общ. ред. А.В. Федорова, В.Н. Цыгичко. – М.: ПИР-Центр, 2001. – С. 72-77.

[17] Основные работы: Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты / Г.В. Грачев. – М.: Институт психологии РАН, 1996; Ермаков Ю.А. Манипуляция личностью: смысл, приемы, последствия / Ю.А. Ермаков. – Екатеринбург, 1995; Лепский В.Е. Глобальное информационное общество и информационная безопасность России: проблема становления стратегических субъектов / В. Е. Лепский // http://www.yandex.ru/yandsearch?stype=www&nl=0&text=%CB%E5%EF%F1%EA%E8%E9+%C2.%C5; Лисичкин В.А. Третья мировая (информационно-психологическая) война / В.А. Лисичкин, Л.А. Шелепин – М.: Институт социально-политических исследований АСН, 2000. – 304 с.; Месснер Е. Мятежвойна – это битва за душу воюющего народа / Е.Месснер // Независимое военное обозрение. – 1999. – № 43; Панарин И.Н. Информационная война и власть / И.Н.Панарин. – М.: Мир безопасности, 2001. – 240 с.; Панарин И.Н. Информационная война и мир / И.Н. Панарин, Л.Г. Панарина. – М.: ОЛМА-ПРЕСС, 2003. – 384 с.; Панарин И.Н. Информационная война XXI века: готова ли к ней Россия? / И.Н. Панарин // Власть. – 2000. – № 2.; Почепцов Г.Г. Информационные войны / Г.Г. Почепцов. – М.: Рефилл-бук, 2000; Теплов А.А. Власть в информационную эпоху. Мировая политика: вызовы и альтернативы: Сборник научных статей. Выпуск 1 / Под ред. М.М. Лебедевой. – М.: МГИМО (У) МИД России. – 2003. – С. 145-163.

[18] Основные работы: Батурин Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзишский. – М.: Юридическая литература, 1991; Крылов В.В. Расследование преступлений в сфере информации / В.В. Крылов. – М.: Городец, 1998; Расследование неправомерного доступа к компьютерной информации / Под ред. Н.Г.Шурухнова. – М.: Щит-М, 1999; Черных А.В. Обеспечение безопасности автоматизированных информационных систем (уголовно-правовые аспекты) / А.В. Черных // Советское государство и право. – 1990. – № 6. – С. 118.

[19] Номоконов В. Актуальные проблемы борьбы с киберпреступностью / В. Номоконов // http://www.crime-research.ru/library/Nomokon1.html; Сабадаш В. Компьютерная преступность - проблемы латентности / В. Сабадаш // http://www.crime-research.ru/articles/Sabodash06/; Тропина Т. Активность, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику / Т. Тропина // http://www.crime-research.ru/library/Tropina0104.html.

Результаты исследований в области киберпреступности, проведенных этими авторами, в том числе приводимые ими статистические данные, были использованы в диссертационной работе.

Большой вклад в формирование нового научного направления, связанного с исследованием складывающейся и активно развивающейся в настоящее время новой отрасли права – информационного права – внесли И.Л. Бачило, О.А. Городов, В.А. Копылов, В.Н. Лопатин, М.М. Рассолов[20].

При подготовке диссертационной работы автор отталкивался от результатов проведенного этими исследователями анализа правового регулирования информационных отношений, возникающих в области обеспечения информационной безопасности, в том числе проблем ответственности за правонарушения в информационной сфере, классификации таких правонарушений.

Вопросами информационных войн занимались такие зарубежные исследователи, как Дж. Аркилла, Д. Деннинг, М. Либики, Л. Пенг, Д. Ронфельд, Т. Томас, Д. Фулгем, У. Швартау, Дж. Штайн[21].

В диссертационной работе исследуются, в частности, причины трансформации содержательного наполнения понятий «информационная война» и «информационные операции», используемых в работах М. Либики и официальных документах Минобороны США.

---

[20] Бачило И.Л. Информационное право / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов; Под ред. Б.Н. Топорнина. – СПб.: Юридический центр Пресс, 2001; Городов О.А. Основы информационного права России / О.А. Городов. – СПб.: Юридический центр Пресс, 2003. – 305 с.; Копылов В.А. Информационное право / В.А.Копылов. – М.: Юристъ, 2002; Рассолов М.М. Информационное право / М.М. Рассолов. – М.: Юристъ, 1999. – 400 с.

[21] Основные работы: Arquilla J. Cyberwar and Netwar: New Models, Old Concepts of Conflict / J. Arquilla, D. Ronfeldt // http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/cyberwar.html; Arquilla J. Cyberwar is coming! / J. Arquilla, D. Ronfeldt // gopher://gopher.well.sf.ca.us/00/Military/cyberwar; Arquilla J. Networks, Netwars and the Fight for Future / J. Arquilla, D. Ronfeldt // http://www.firstmonday.dk.issues/issue6_10/ronfeldt/; Denning D. Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing Foreign Policy / D. Denning // J.Arquilla, D. Ronfeldt Networks and Netwars. – Rand, 2001; Fulghum D. Network Wars / D. Fulghum // Aviation Week & Space Technology. – 2004. – 25 October; Libicki M.C. Incorporating information technology in defense planning / M.C. Libicki // New challenges, new tools for defense decisionmaking. Ed. by S. Johnson, M. Libicki, G.F. Treverton. – RAND, 2003. – PP. 103-131 // http://www.rand.org/pubs/monograph_reports/MR1576/MR1576.ch4.pdf; Peng L. Trusted recovery and defensive information warfare / L. Peng. – Boston: Kluwer Academic Publishers, 2002; Schwartau W. Information warfare: chaos on the electronic superhighway / W. Schwartau. – N.Y.: Thunders Month Press, 1994; Thomas T.L. Deterring information warfare: A new strategic challenge / T.L. Thomas // Parameters. – 1996-1997. – XXV – № 4. – P. 81-91; Stein G. U.S. Information warfare / G. Stein. – Alexandria: Jane's Information Group, 1996.

При том, что отдельные составляющие проблематики информационной безопасности уже в значительной степени подверглись научному осмыслению (например, технические и правовые вопросы борьбы с киберпреступностью, стратегия и тактика ведения информационный войн), на сегодняшний день практически не существует предметных исследований международной информационной безопасности с учетом всех ее основных составляющих и угроз, реализующихся или потенциально имеющихся в этой сфере; отсутствуют системные исследования подходов и механизмов, направленных на обеспечение инфобезопасности, а также комплексные разработки в области применимости действующей политико-правовой базы к сфере международной информационной безопасности (МИБ) и ее достаточности для регулирования возникающих в ней отношений. Как следствие – не выработаны и не обоснованы дальнейшие направления укрепления международной информационной безопасности.

В диссертационной работе *объектом исследования* является международная информационная безопасность – состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве.

Предмет исследования – политические проблемы обеспечения международной информационной безопасности.

Диссертация преследует следующую *основную цель* – исследовать основные политические проблемы обеспечения международной информационной безопасности и определить возможные и целесообразные пути и средства ее укрепления.

В исследовании ставятся следующие *основные задачи*:

- рассмотреть в комплексе основные угрозы международной информационной безопасности, описать их недостаточно изученные проявления и проанализировать их возможные последствия;
- исследовать направления и содержание международного сотрудничества и переговорного процесса в области МИБ и международные подходы к обеспечению информационной безопасности, выработанные или находящиеся в стадии разработки в рамках международных и региональных

организаций и форумов, и оценить их эффективность и адекватность задачам снижения существующих угроз в этой сфере;

- проанализировать действующие международные политико-правовые документы и механизмы, относящиеся к информационной безопасности, с целью определения их достаточности для регулирования вопросов обеспечения международной информационной безопасности;
- выявить возможные и целесообразные пути и средства укрепления международной информационной безопасности.

Методологической основой исследования является сочетание элементов системного, конкретно-исторического, компаративного анализа, контент-анализа и анализа статистических данных, методов индукции и дедукции.

Использование в работе этих методов позволило комплексно рассмотреть основные политические проблемы обеспечения международной информационной безопасности, в частности проанализировать основные угрозы МИБ, исследовать действующие международные политико-правовые документы и многосторонние подходы, направленные на снижение этих угроз и укрепление международной информационной безопасности, а также наметить дальнейшие пути и средства обеспечения международной информационной безопасности.

Применение элементов системного анализа позволило представить объект изучения – международную информационную безопасность – в его единстве и целостности и на этой основе определить дальнейшие направления обеспечения МИБ. В работе были рассмотрены основные политические, экономические, социально-культурные и технологические последствия информатизации. В качестве основных угроз в сфере международной информационной безопасности были выделены и исследованы киберпреступность, информационный терроризм – как самостоятельный вид преступной деятельности, отличающийся от киберпреступности прежде всего своей политической направленностью, которая свойственна терроризму в целом – и информационные войны, оказывающие наибольшее влияние на современную систему международных отношений.

Объект исследования в диссертации рассматривается в первую очередь в политологическом ключе. Вместе с тем он носит многофакторный характер и

включает в себя в качестве неотъемлемого элемента правовую компоненту, что обусловило необходимость использования в работе междисциплинарного подхода. Анализ существующих международных политико-правовых документов и механизмов обеспечения международной информационной безопасности с точки зрения охвата ими трех основных составляющих МИБ дал возможность определить возможные пути и средства ее дальнейшего обеспечения.

При подготовке диссертации в качестве *основных источников информации* использовались международные политико-правовые документы; политические документы, а также нормативные и иные правовые акты Российской Федерации; информационные материалы; статистическая информация; прогнозы и документы международных организаций; научная и аналитическая литература; газетные и журнальные публикации в специализированных изданиях; научные публикации, размещенные в Интернет; доклады на конференциях и семинарах; интервью с представителями федеральных органов исполнительной власти Российской Федерации и экспертами в области информационной безопасности, а также собственные публикации автора.

Новизна работы определяется, прежде всего, тем, что в ней предпринята попытка многофакторного и междисциплинарного рассмотрения проблематики международной информационной безопасности с вычленением основных угроз и факторов, влияющих на ее обеспечение.

В диссертации исследованы основные политические проблемы обеспечения международной информационной безопасности, проанализированы направления и содержание международного сотрудничества и переговорного процесса в области международной информационной безопасности и многосторонние подходы к решению этой проблемы во всех ее аспектах, выработанные или находящиеся на настоящий момент в стадии разработки в международных организациях и в рамках международных форумов, проведена оценка их действенности и адекватности задачам снижения существующих угроз в этой сфере.

На основании результатов анализа применимости действующей международной политико-правовой базы к сфере международной информационной безопасности и ее достаточности для регулирования этой сферы, дана оценка

перспективности продолжения консультативного и переговорного процессов по этой проблематике на двустороннем, региональном и международном уровнях; определены целесообразные пути и средства дальнейшего укрепления МИБ, при этом выявлена приоритетность вопросов, по которым возможно достижение международных договоренностей.

Исследование базируется на самых последних данных о процессах информатизации в мире и в России. В работе используются результаты самых современных исследований российских и зарубежных авторов, посвященных анализу политических, военных, экономических и других аспектов информатизации.

Теоретическая значимость работы определяется, прежде всего, тем, что в ней осуществлено комплексное исследование политических проблем обеспечения МИБ с учетом угроз военно-политического, преступного и террористического характера и возможностей для ее дальнейшего международного политического и правового закрепления.

Обобщены, систематизированы и проанализированы результаты последних научных исследований в области информатизации, информационного общества, психологических и информационных войн, информационного права, международных отношений и процессов глобализации.

Практическая значимость работы определяется тем, что ее основные положения были использованы при выработке элементов государственной политики Российской Федерации в области продвижения российской инициативы по международной информационной безопасности в ООН, других международных организациях, на международных форумах и в региональных организациях, в частности в рамках Шанхайской организации сотрудничества, в ходе работы над проектом международно-правового документа по МИБ, при подготовке тактических и позиционных документов к международным двусторонним и многосторонним консультациям и заседаниям Группы правительственных экспертов ООН по международной информационной безопасности, состоявшимся в 2004-2005 годах.

Результаты диссертационного исследования могут быть использованы в учебном процессе, при подготовке общих и специальных курсов, учебных пособий по данной теме.

Структура диссертации

Диссертация состоит из введения, трех глав, заключения и библиографии. Основной текст изложен на 183 страницах. Избранная структура диссертации обеспечивает возможность последовательного и системного анализа предмета исследования и решения поставленных в диссертации задач, которые перечислены во введении.

Ниже приводится оглавление работы.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Введение

Во введении приводится общая характеристика работы, раскрывается актуальность исследования политических проблем обеспечения международной информационной безопасности, определяются объект и предмет исследования.

Значительное внимание уделяется вопросу разработанности проблемы диссертационного исследования, анализу существующего задела исследовательских материалов. В этом разделе введения приводится обзор основных российских и зарубежных источников, которые используются в диссертации.

Отмечается, что, хотя в настоящее время имеются работы по тем или иным аспектам информационной безопасности, проблематика международной информационной безопасности в комплексе по-прежнему остается малоизученной в России и за рубежом; аргументируется новизна исследования.

Описывается методологическая основа исследования, обосновываются преимущества применения тех или иных методологических подходов для решения поставленных задач.

Представлены теоретическая и практическая значимость работы, информация об апробации результатов диссертации, а также приведены основные положения, выносимые автором на защиту.

Глава 1. Сущность проблемы и угрозы международной информационной безопасности

В первой главе рассматривается существо проблемы международной информационной безопасности; дается оценка ее значимости для обеспечения международной безопасности; определяются основные факторы, влияющие на ее состояние; комплексно рассматриваются, классифицируются и описываются основные угрозы международной информационной безопасности, исследуются их недостаточно изученные проявления и анализируются их возможные последствия.

В разделе 1.1 выделяются основные угрозы, субъекты и объекты международной информационной безопасности. Обосновывается опасность угроз МИБ для всей системы международной стабильности и безопасности, для социально-политического развития отдельных государств.

Акцент в этом разделе делается на вопросах использования ИКТ в преступных целях. Приводятся рабочее определение киберпреступности, классификация киберпреступлений; отмечаются их основные особенности; анализируются наиболее опасные случаи кибернападений, в том числе вирусные эпидемии, блокирующие нормальную работу Интернет, атаки на критические инфраструктуры. Выявляется связь между терроризмом и киберпреступностью. Подчеркивается высокий потенциал воздействия киберпреступлений на международную безопасность.

В разделе 1.2 подробно исследуется проблема использования ИКТ в террористических целях. Кибертерроризм выделен в отдельный раздел работы, поскольку, являясь один из видов киберпреступности, он имеет иные, свойственные терроризму в целом, цели и представляет собой особо опасную разновидность преступной деятельности.

Приводится рабочее определение кибертерроризма, анализируются основные приемы, которые могут использоваться для достижения террористических целей в информационном пространстве; выделены объекты кибертерроризма; изучены его особенности; проанализирован феномен психотерроризма. Ставится вопрос о том, что враждебные военно-политические или являющиеся по существу террористическими действия, целенаправленно ведущиеся одним государством

против другого, могут быть замаскированы под деятельность международных террористов, не имеющих государственной принадлежности, причем в таких случаях выявление истинного источника атаки и соответствующее реагирование на нее может стать чрезвычайно сложным или даже невозможным. Делается вывод о том, что в силу высокой поражающей способности и скрытности источника воздействия кибертерроризм может стать катализатором или триггером региональных и глобальных конфликтов.

Раздел 1.3 посвящен анализу спектра вопросов, связанных с применением ИКТ в качестве оружия. В этом разделе приводится рабочее определение информационного оружия, исследуются и систематизируются его свойства, представлена классификация и основные особенности информационного оружия и типов информационной войны, выявляются объекты и цели информационной войны. Подробно исследуются негативные геополитические последствия появления, применения и распространения информационного оружия для системы современных международных отношений. Анализируется враждебное военно-политическое использование ИКТ в ходе последних вооруженных конфликтов и в преддверии их, а также проведение информационных операций в мирное время.

Основной вывод, вытекающий из анализа, представленного в первой главе, заключается в том, что весьма опасный характер угроз МИБ делает противодействие им важным аспектом укрепления национальной, региональной и международной безопасности и стратегической стабильности, а вследствие этого – значимым фактором современной мировой политики.

Глава 2. Международное сотрудничество и переговорный процесс в области международной информационной безопасности

Вторая глава посвящена подробному исследованию направлений и содержания международного сотрудничества и переговорного процесса в области МИБ и основных подходов, выработанных или находящихся в стадии разработки в рамках международных и региональных организаций и форумов, к обеспечению международной информационной безопасности, и оценке их эффективности и адекватности задачам снижения существующих угроз в этой сфере.

В разделе 2.1 анализируются основные этапы и задачи продвижения Россией инициативы международной информационной безопасности в ООН, в рамках которого с 1998 года в Первый комитет ГА ООН российской стороной вносятся проекты резолюций «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (№№ 53/70, 54/49, 55/28, 56/19, 57/53, 58/32, 59/61, 60/45). Приводятся позиции ключевых стран относительно предлагаемых Россией путей и средств укрепления МИБ.

В разделе 2.2 изучаются инициативы США в области информационной безопасности в рамках Второго и Третьего комитетов Генассамблеи ООН, которые ориентированы на борьбу с киберпреступностью, обеспечение защиты критических информационных инфраструктур и создание глобальной культуры кибербезопасности. В этом разделе анализируются резолюции ГА ООН, принятые по этим вопросам по предложению США (№№ 55/63, 56/121, 57/239, 58/199).

В разделе 2.3 рассматривается ход обсуждения проблемы информационной безопасности в рамках «Группы восьми», в частности в Лионской/Римской Группе и ее Подгруппе по преступлениям в сфере высоких технологий, в круг ведения которых входят такие вопросы, как борьба с преступностью и терроризмом в киберпространстве, защита критических информационных инфраструктур, обеспечение безопасности операций электронного бизнеса и электронной торговли. Анализируются положения Окинавской хартии – первого документа, принятого на уровне глав государств и посвященного вопросам глобального информационного общества, – в части, касающейся информационной безопасности.

Раздел 2.4 посвящен изучению международных подходов, выработанных в Международном союзе электросвязи (МСЭ) и на Всемирной встрече на высшем уровне по вопросам информационного общества (ВВУИО). Анализируются итоговые документы руководящих органов МСЭ, региональных конференций по подготовке к ВВУИО, первого и второго этапов саммита по информационному обществу.

В разделе 2.5 рассматривается международная деятельность по обеспечению информационной безопасности, осуществляемая в рамках некоторых региональных организаций и специальных международных организаций – в СНГ, ЕС, АТЭС, ОАГ, ОЭСР.

Анализ международного переговорного процесса по вопросам, связанным с информационной безопасностью, результаты которого приведены во второй главе, позволяет сделать вывод об уникальности российской инициативы по МИБ. Только она предусматривает многоаспектное и всестороннее обеспечение информационной безопасности на глобальном уровне в привязке к триаде угроз военно-политического, криминального и террористического характера.

Продвигаемые в ООН инициативы США по кибербезопасности ориентированы прежде всего на универсализацию соответствующих мер, принимаемых этим государством или при его участии и отвечающих его национальным интересам. Они направлены на сугубо технологическое, «внутреннее» укрепление безопасности компьютерных и сетевых средств без учета угроз внешнего характера, причем с использованием американских методик и средств, что может сделать информационное пространство зарубежных стран для США проницаемым и контролируемым. Международное сотрудничество сводится лишь к обмену информацией и передаче технологий киберзащиты.

В других международных организациях рассматриваются отдельные частные аспекты информационной безопасности (борьба с киберпреступностью, противодействие кибертерроризму, создание культуры кибербезопасности), а принимаемые ими документы либо носят сугубо декларативный характер, либо ограничены по своей географии и сфере применения. Ни в одной из вышеперечисленных организаций помимо ООН военно-политическая компонента МИБ не рассматривается.

Глава 3. Анализ международной политико-правовой базы в области информационной безопасности

В третьей главе рассматриваются вопросы применимости действующей международной политико-правовой базы к сфере МИБ и раскрываются позиции стран, являющихся ключевыми игроками на информационно-коммуникационном поле, относительно возможности применения современного международного права к области информационной безопасности и его достаточности для регулирования возникающих в ней отношений. Целью этого исследования является выявление

принципиальной необходимости, а также путей и средств дальнейшего развития международного консультативного и переговорного процессов по международной информационной безопасности, а также политико-правовой базы, относящейся к сфере МИБ.

В этих целях в разделе 3.1 анализируются основополагающие принципы международного права, в том числе закрепленные в Уставе ООН.

В разделе 3.2 основное внимание уделяются праву вооруженных конфликтов и международному гуманитарному праву.

В разделе 3.3 приводится политико-правовой анализ международных документов в области борьбы с терроризмом.

Результаты исследования, проведенного в разделах 3.1 – 3.3, свидетельствуют о том, что информационное противоборство в полной мере не регулируется действующими международными политико-правовыми документами, что связано с радикально отличным характером враждебного применения информационных технологий и средств от параметров традиционных боевых и террористических действий.

В разделе 3.4 на основе результатов проведенного в диссертации анализа намечаются дальнейшие пути и средства обеспечения МИБ. Выявляется приоритетность вопросов, по которым возможно достижение международных договоренностей. Приводятся целесообразные, по мнению автора, стратегия и тактика дальнейшего продвижения консультативного и переговорного процессов по МИБ на двустороннем, региональном и международном уровнях. Предлагаются основные элементы, которые могли бы быть инкорпорированы в перспективный политико-правовой документ, такой как принципы деятельности или кодекс поведения государств в области международной информационной безопасности, а в перспективе – в проект юридически обязательного международного договора, регулирующего отношения в области международной информационной безопасности.

Положения, выносимые на защиту:

- Стремительное развитие и использование информационно-коммуникационных технологий и средств в глобальном масштабе имело решающее значение для перехода от индустриального к постиндустриальному, информационному, обществу, открывающему широчайшие позитивные возможности для прогрессивного развития человека, общества, государства и международного сообщества в целом, достижения устойчивого экономического роста, распространения процессов демократизации, укрепления гражданского общества.

- Глобальная информатизация может в ряде случаев прямо или опосредованно приводить к негативным последствиям: усугублению «цифрового разрыва», которое может повлечь за собой дальнейшую поляризацию мира, размыванию понятия суверенитета государств, нарушению основных прав и свобод человека в информационной сфере, подрыву национальной безопасности государств, манипуляции общественным сознанием.

- Сформировавшаяся за последние полтора десятилетия фундаментальная зависимость от нормального функционирования информационно-коммуникационных технологий гражданских и военных инфраструктур государств, в том числе критических, а также возможность использования ИКТ в преступных, террористических и враждебных военно-политических целях дали толчок для возникновения принципиально новых – информационных – угроз международной безопасности и стратегической стабильности. Информационное оружие способствует усилению военного потенциала использующих его государств, а его применение может иметь последствия, сопоставимые с последствиями применения оружия массового уничтожения.

- Существующие многосторонние механизмы, направленные на обеспечение информационной безопасности, недостаточны для эффективного решения вопросов международной информационной безопасности, адекватного угрозам в этой сфере. Подход, предусматривающий многоаспектное и всестороннее обеспечение информационной безопасности на национальном, региональном и глобальном уровнях в привязке к триаде угроз военно-политического,

криминального и террористического характера, предусматривается лишь российской инициативой по МИБ.

- Вопросы регулирования сферы информационного противоборства в полной мере не подпадают под действие ни одного из существующих на сегодняшний день международных политико-правовых документов. Документы, так или иначе затрагивающие проблематику международной информационной безопасности, либо оказываются недопустимо суженными по своему предмету и/или географическому охвату, либо допускают множественность трактовок основных понятий. Соответствующие национальные законодательства являются недостаточными как в силу трансграничности ИКТ, так и в силу своей разнородности и недостаточно высокой степени гармонизации.

- Эффективное противодействие угрозам в информационной сфере возможно за счет кодификации и прогрессивного развития соответствующих норм международного права для обеспечения эффективного регулирования отношений, возникающих в информационном пространстве, на базе продолжения консультативного и переговорного процессов на двустороннем, региональном и международном уровнях, в том числе путем выработки и принятия нового политико-правового документа, такого как принципы деятельности или кодекс поведения государств в области международной информационной безопасности, многостороннего договора о борьбе с информационным терроризмом, а в перспективе – юридически обязательного международного договора, регулирующего отношения в области международной информационной безопасности.

Апробация результатов исследования.

Основные положения и выводы диссертационной работы докладывались автором в ходе конференций и семинаров по вопросам информационной безопасности, в том числе на 6-ой Всероссийской конференции «Информационная безопасность России в условиях глобального информационного общества» (ИНФОФОРУМ), на совместном семинаре ПИР-Центра политических исследований и Фонда гражданских инициатив в политике Интренет «Трансформация понятия

информационная безопасность в информационную эпоху» и др., а также опубликованы автором в следующих изданиях:

Сафронова И.Л. Информационная безопасность: основные проблемы и перспективы / И.Л. Сафронова // Вопросы защиты информации. – 2006. – № 2 (73). – С. 35-39.

Сафронова И.Л. Международное сотрудничество в области информационной безопасности / И.Л. Сафронова // Инфофорум. Бизнес и безопасность в России. – 2004. – № 38. – С. 92-98 // http://www.infoforum.ru/detail.php?pagedetail=868.

Сафронова И.Л. Информационная безопасность: основные проблемы и перспективы / И.Л. Сафронова // Промышленная политика в Российской Федерации. – Сдано в печать.

Сафронова И.Л. Основные угрозы информационной безопасности и целесообразные пути их снижения / И.Л. Сафронова // Вестник компьютерных и информационных технологий. – Сдано в печать.

Технологический прогресс и современные международные отношения: Учебник для ВУЗов / Под общ. ред. А.В. Крутских. – М.: Просвещение, 2004. – 448 с.

Krutskikh A.V. International Cooperation in the Field of Information Security / A.V. Krutskikh, I.L. Safronova // Partnership for Peace Consortium of Defense Academies and Security Studies Institutes Journal. – Сдано в печать.

Результаты диссертационной работы использовались при проведении спецкурса по научно-технологической составляющей международных отношений в рамках лекционного процесса в МГИМО (У) МИД России.

МГИМО (У) МИД России
Заказ №312 Тираж 100 экз.

Отпечатано в отделе оперативной полиграфии
и множительной техники МГИМО (У) МИД России
119218, Москва, ул. Новочеремушкинская, 26