Первому геополитику России
Михаилу Васильевичу Ломоносову
по случаю 300-летия со дня рождения
посвящается

ГЛОБАЛЬНАЯ БЕЗОПАСНОСТЬ: ИННОВАЦИОННЫЕ МЕТОДЫ АНАЛИЗА КОНФЛИКТОВ

Под общей редакцией
Председателя отделения «Информационная глобализация»
Российской академии естественных наук,
доктора исторических наук, профессора

А.И.СМИРНОВА

Общество «Знание» России
Москва
2011

ББК 66.2
УДК 327
С 50

Рецензенты:
Доктор исторических наук, профессор Дахин В.Н.
Доктор экономических наук, профессор Аникин В.И.

Авторский коллектив:
д.и.н. А.И.Смирнов (введение, гл.1, 2, §§ 3.1., 3.7, 3.8, 5.1, 5.3, 5.4., заключение)
д.э.н. А.И.Агеев, к.в.н. Б.В.Куроедов, О.В.Сандаров (§ 4.4.)
д.т.н. В.С.Кретов, Н.М.Котов, аспирант РАГС М.Н.Котов (§§ 3.6, 4.1, 4.2., 4.3.)
к.п.н. И.Н.Кохтюлина (§§ 3.2., 3.3., 3.4., 3.5., 5.2.)

Глобальная безопасность: инновационные методы анализа конфликтов. Под общ.ред. Смирнова А.И. – М.: Общество «Знание» России. 2011. - 272 с.

ISBN 978-5-254-02022-6

В условиях стремительных процессов глобализации усилия политологов по анализу и, особенно, прогнозированию конфликтов на основе традиционных методов обречены (при всем уважении к их интеллекту, опыту и интуиции), как правило, лишь на краткосрочный эффект. Экспертное сообщество всего мира пытается найти инновационные решения оптимальных вариантов кризисного реагирования. Настоящая книга - это попытка кратко дать понятийный аппарат основных проблем и трендов глобальной безопасности, традиционных методов анализа конфликтов, а основное внимание уделить инновационным.

Книга позиционирует новейшие теоретические и практические наработки на стыке современных информационно-коммуникационных технологий (ИКТ): ситуационно-кризисных центров (СКЦ), информационно-аналитических и геоинформационных систем и т.д. и проблем глобальной безопасности для оптимального кризисного реагирования на них и прогнозирования.

С учетом динамично расширяющегося арсенала СКЦ и ИКТ в международной конфликтологии работа может быть полезна для широкого круга читателей, интересующихся столь актуальными направлениями мировой политики.

Anatoly I. SMIRNOV
Global safety: innovative methods of the analysis of conflicts.

In the conditions of prompt processes of globalization of effort of political scientists under the analysis and, especially, forecasting of conflicts on the basis of traditional methods are doomed (at all respect for their intelligence, experience and intuition), as a rule, only to short-term effect. The expert community of the whole world tries to find innovative decisions of optimum variants of crisis reaction. The present book is attempt to give short the conceptual device of the basic problems and trends of the global safety, traditional methods of the analysis of conflicts, and the basic attention to give to the innovative.

The book positions the newest theoretical and practical operating time on a joint of modern information-communication technologies (ICT): the situation (crisis) centers, information-analytical and geoinformation systems etc. and problems of global safety for optimum crisis reaction to them and forecasting.

Taking into account dynamically extending arsenal of situation (crisis) centers and ICT in the international conflictology the book can be useful for laymen, the interested so actual directions of world politics.

ISBN 978-5-254-02022-6

К ЧИТАТЕЛЮ

Усложняющаяся матрица глобальной безопасности императивно требует инновационных ответов на ее вызовы. Данная работа, предпринятая членами постоянной Экспертной комиссии «Ситуационные центры и аналитические решения для государственного управления» национального ИНФОФОРУМА и Национального института исследований глобальной безопасности (НИИГлоБ), является попыткой адекватного анализа столь важной проблемы для судеб цивилизации. Следует отметить, что в последнее время в международной и отечественной практике предпринимаются отдельные попытки рассмотреть сложнейшие международные процессы с использованием современных информационных технологий, в т.ч. контент-, ивент- и коннект-анализа. Однако эти исследования все-таки страдают описательностью и отсутствием прогностического компонента.

К очевидным достоинствам книги следует отнести то, что наряду с инновационными методами исследования глобальной безопасности во всех ее измерениях авторы весьма кратко, но емко освещают традиционные методы, а также приводят прикладные исследования по природогенным, техногенным и социогенным катастрофам, международной информационной безопасности, проблематике раздела арктических пространств. Интересен подход к анализу идейных и финансовых источников международного терроризма как разновидности ассиметричной войны.

Безусловно, полезным для читателей будет глоссарий, а также систематизированная международно-правовая информация в приложении.

Председатель постоянной Экспертной комиссии
«Ситуационные центры и аналитические решения
для государственного управления»
национального ИНФОФОРУМА,
заместитель Руководителя
Росфинмониторинга  А.М.Спиридонов

СОДЕРЖАНИЕ

CONTENTS

Задача дипломатической службы -
придать своей работе новое качество….
необходим глубокий аналитический
подход к событиям прогнозирования
тенденций развития как двусторонних,
так и многосторонних отношений.[1]

Д.А.МЕДВЕДЕВ, 12 июля 2010 г.

ВВЕДЕНИЕ

Завершилось первое десятилетие XXI века. Оно по праву может войти в скрижали человечества как одно из самых драматичных. Сполохи войны цивилизаций в виде международного терроризма и мирового финансово-экономического кризиса, рецидивы холодной войны и пиратства, всплеск локальных и региональных конфликтов, техногенные катастрофы и климатические катаклизмы, эпидемии и пандемии и, наконец, беспрецедентная утечка секретной дипломатической переписки США на Wikileaks - вот далеко не полный перечень его трагедий.

Наиболее емко сложившаяся ситуация оценена в Стратегии национальной безопасности России (от 12 мая 2009 г.): «Возросла уязвимость всех членов международного сообщества перед лицом новых вызовов и угроз» [2].

Попытки осмысления и прогнозирования глобальных катаклизм предпринимает интеллектуальная элита всего мира. В этом контексте минувшее столетие достаточно условно делится на следующие **три** этапа[3].

Первый - начало мировой войны, революция в России, неправедный Версальский мир, первая «холодная война», сталинизм, фашизм, Вторая мировая война.

Второй - победа над фашизмом, создание ООН и Бреттон-вудской системы управления мировыми финансами, биполярный мир, разрядка, «холодная война», перестройка в СССР.

Третий - поражение коммунизма, развал СССР, однополярный мир под эгидой США, принижение роли ООН, провал завышенных надежд России на рынок и демократизацию (обостренный кризи-

[1] http://www.mid.ru/brp_4.nsf/0/21187082074FD703C325775F001E6D58
[2] http://www.scrf.gov.ru/documents/99.html
[3] См. http://cceis.ru/rus/analitic/83.html

сами на постсоветском пространстве), периферийность «третьего мира», дезинтеграция системы международной безопасности, «гуманитарная интервенция» в Югославию, экспансия НАТО на Восток, всплеск международного терроризма.

При этом «победивший» Запад не создал системы глобальной безопасности, допустил распространение ядерного оружия (в т.ч. и в балансирующих на гране войны Индии и Пакистане), не решил ближневосточной проблемы, вторгся в Ирак и в Афганистан, признал независимость Косово, поддержал военно-политический авантюризм руководства Грузии, совершил еще ряд досадных ошибок.

МВФ и иные финансовые институты слепо следовали рецептам «Вашингтонского консенсуса» и суперлиберальной англосаксонской модели, что и привело к глобальной рецессии.

Вместе с тем кризис способствовал «перезагрузке» российско-американских и иных форматов международного сотрудничества. Это содействовало определенному потеплению климата международных отношений, что создает хорошие предпосылки для реализации курса российской дипломатии на обеспечение благоприятных внешних условий в интересах инновационного развития страны и укрепления модернизационных партнерств с наиболее развитыми государствами Европы, Америки и Азиатско-Тихоокеанского региона.

Результаты состоявшихся в ноябре-декабре 2010 г. саммитов Совета Россия-НАТО в Лиссабоне и ОБСЕ в Астане, начавшийся процесс ратификации договора об СНВ-3 подтвердили безальтернативность качественного улучшения ситуации в евроатлантических делах, утверждения на практике принципов неделимой и равной безопасности. Сейчас стоит задача закрепления достигнутого, недопущения негативного воздействия на общие интересы любой внутриполитической конъюнктуры.

При этом, как отметил Д.А.Медведев на торжественном собрании, посвященном 90-летию Службы внешней разведки России 15 декабря 2010 г., «…тот глобальный информационный поток, в который оказался погружен наш земной шар, существенно изменил систему принятия решений, создал новые проблемы»[4].

В этом контексте, свою монографию[5] (неожиданно удостоенную медалью и дипломом 9-й всероссийской конференции «ИНФОФОРУМ» в номинации «публикация года» (2007 г.) я завершил параграфом «Императив информационной глобализации для России:

[4] http://www.kremlin.ru/news/9825

[5] Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности.- М.2005. «Парад»

инновационная конкурентоспособность». В книге, в частности, приведен рассекреченный в 2005 г. документ[6], подготовленный по заказу ЦРУ, «Контуры мирового будущего: доклад по проекту - 2020»[7]. Его суть сводится к следующему.

1. **«Давосский мир»** - экономический рост, во главе которого встанут Китай и Индия, способен в ближайшие 15 лет изменить направление процессов глобализации, придав им менее западный облик.

2. **Pax Americana** - США сохраняют свою доминирующую роль при радикальных изменениях мирового политического пейзажа и смогут повлиять на формирование нового мирового порядка.

3. **New Caliphate** - радикальная религиозная политика бросает вызов западным нормам и ценностям, становясь фундаментом новой системы.

4. **«Кольцо страха»** - обеспокоенность распространением ОМП может привести к крупномасштабным превентивным интервенциям (как в Ираке), результатом которых может стать создание оруэлловского мира.

Попытку дать свое видение развития России сделал А.Шубин «Россия-2020: будущее страны в условиях глобальных перемен»[8], где автор предлагает три сценария, суть которых сводится к следующему:

1. **«Конец истории»** - глобализация справилась с новыми вызовами. Россия интегрировалась в нее в качестве периферии, а ее элита - в мировую элиту на подчиненных ролях. Сетевые структуры подчинены глобальной информационной олигархии, контролирующей институты мирового правительства.

2. **«Великие потрясения»** - глобальный рынок рухнул, началась новая Великая депрессия, произошло выравнивание уровня жизни стран Запада и среднеразвитых стран, в мире нарастает волна революций и этно-конфликтов. Российская элита, не готовая к таким событиям, смещается массовыми выступлениями. Сценарий открывает возможность для мировой гегемонии традиционистских проектов, а для России - вариант «догоняющего развития».

3. **«Третья волна во втором эшелоне»** - в России формируется социально-креативный постиндустриальный уклад, полномочное

---

6 http://www.from-ua.com/politics/42493dd1c215d/

7 Первый аналогичный материал вышел в 1997 г. под названием «Глобальные тенденции» (до 2010 года), второй - «Глобальные тенденции-2015», о четвертом (вышел в конце 2008 г. - «Глобальные тенденции-2025: изменившийся мир»), см. в заключении

8 Россия и мир в 2020 году: Доклад Национального разведывательного совета США «Контуры мирового будущего». А.Шубин. «Россия-2020: будущее страны в условиях глобальных перемен». М. Европа. 2005. 218 С.

самоуправление, защита и поддержка гражданского общества и корневых информационных структур. В этих интересах возможно использование «неосоветского возрождения снизу», а также опыта стран «первого эшелона» в преодолении «третьей волны», что существенно облегчит задачи России.

Следует отметить, что мои комментарии к данным сценариям вызвали значительный интерес как читателей[9], так и различных аудиторий.

В силу этого и появилась мысль написать книгу-продолжение, где кратко изложить понятийный аппарат проблем и трендов глобальной безопасности, традиционные методы анализа международных конфликтов, а основное внимание уделить инновационным.

Действительно, в условиях стремительных процессов глобализации усилия экспертов (при всем уважении к их интеллекту, опыту и интуиции) по анализу и, особенно, прогнозированию конфликтов на основе традиционных методов обречены, как правило, лишь на краткосрочный эффект.

В этом плане следует отметить, что в качестве сотрудника Международного отдела ЦК КПСС мне довелось участвовать в ряде ситуационных анализов во второй половине 1980-х гг. Не могу не отметить в позитивном ключе данный метод, разработанный Е.М.Примаковым, В.И.Гантманом и В.И.Любченко еще в 1970-е гг.[10]

Характерно, что на базе этого метода ведущие эксперты все более активно используют ситуационно-кризисные центры (СКЦ), оснащенные новейшими информационно-коммуникационными технологиями (ИКТ). СКЦ и их информационно-аналитические системы позволяют в он-лайне вести мониторинг, контент,- ивент- и коннект-анализ, в т.ч. мультимедийной информации на иностранных языках о «горячих точках» в мире, прогнозировать их возникновение и развитие, а также, опираясь на базы знаний, вносить лицу, принимающему решение (ЛПР), оптимальные предложения по реагированию на них (в т.ч. с визуализацией).

С учетом динамично расширяющегося арсенала СКЦ и ИКТ в международной конфликтологии одному справиться со столь амбициозным планом написания данной книги было бы крайне сложно.

[9] Кроме быстро разошедшегося тиража книги (3000 шт.), ее электронная версия, выставленная на сайте www.polpred.ru, за три года была скачена свыше 8000 раз

[10] См. Примаков Е.М. Методика и результаты ситуационных анализов. Мастер-класс по программе Мировая политика. МГИМО(У). 2006

В силу этого очень рад сотрудничеству с коллегами «по цеху», которые высокопрофессионально осветили в ней свои треки.

Что касается структуры книги, то в целом она базируется на циклах моих лекций в Дипломатической академии МИД России по спецкурсам «Проблемы национальной безопасности» и «ИКТ в госуправлении», а также в МГИМО(У) при МИД России «Современные информационные технологии в дипломатической практике». Кроме того, использован опыт выступлений в качестве члена Федеральной лекторской группы общества «Знание» и члена оргкомитета Национального форума по информационной безопасности «ИНФОФОРУМ».

Следует подчеркнуть, что в последнее время рядом отечественных и зарубежных экспертов были предприняты попытки по-новому посмотреть на данную проблему. Особо актуальны работы В.И.Аникина, Е.Г.Барановского, Н.Н.Владиславлевой, А.Д.Богатурова, Л.Блумфильда, Т.Ванханена, Л.В.Дериглазовой, Е.В.Колдуновой, Б.Н.Кузыка, В.М.Кулагина, М.М.Лебедевой, А.Ю.Мельвиля, А.И.Никитина, М.А.Хрусталева, П.А.Цыганкова, Р.А.Явчуновской, Ю.В.Яковца[11] и др.

В этом контексте очень полезными стали материалы V конвента РАМИ под общей редакцией ректора МГИМО (У), акад. РАН А.В.Торкунова[12], его труд «По дороге в будущее» [13], а также работы авторских коллективов РАГС под общей редакцией В.А.Михайлова и В.С.Буянова «Международная безопасность России в условиях

[11] См. Аникин В.И. Теория и практика управления во внешнеполитической деятельности.- М.1999; Барановский Е.Г., Владиславлева Н.Н. Методы анализа международных конфликтов. - М.Научная книга. 2002.; Богатуров А.Д. Современная мировая политика: прикладной анализ. Учебное пособие для ВУЗов (изд:2). Аспект-Пресс. 2010; Lincoln Bloomfield and Allen Moulton. Managing International Conflict: From Theory to Policy. New York, 1997. Vanhanen T. Democratization: A Comporative Analysis of 170 countries - L;N.Y.: Routledge, 2003; Дериглазова Л.В. Парадокс ассиметрии в международном конфликте, http://www.intertrends.ru/nineth/007.htm ; Колдунова Е.В. Сравнительный анализ региональных особенностей новых угроз безопасности: учеб.пособие. - М.: Проспект, 2010; Кузык Б.Н. Россия и мир в XX1 веке. – М.2005; Политический атлас современности: опыт многомерного статистического анализа политических систем современных государств. - М.: Изд-во «МГИМО-Университет», 2007.; Лебедева М.М. Международные конфликты в современном мире: их исследование и урегулирование / М.М. Лебедева // Международные отношения : теории, конфликты, движения, организации / Под ред. проф. П.А. Цыганкова. - М.: Альфа-М, Инфра-М. - 2007. Никитин А.И. Конфликты, терроризм, миротворчество.- М. Навона, 2009; Хрусталев М.А. Анализ международных ситуаций и политическая экспертиза: очерки теории и методологии.-М: НОФМО, 2008; Р.А.Явчуновская. Глобальная и региональная безопасность: курс лекций. - М.: Изд-во РАГС, 2010; Яковец Ю.В. Эпохальные инновации XXI века. М.: Экономика, 2004.

[12] http://www.mgimo.ru/convention2008.risa/index.phtml

[13] А.В.Торкунов «По дороге в будущее» / Ред.-сост. А.В.Мальгин, А.Л.Чечевишников. - М.: Аспект Пресс, 2010. - 476 с.

глобализации»[14], Дипломатической академии МИД России под общей редакцией проф. В.И.Анненкова «Военная сила в международных отношениях»[15] и МГИМО(У) под редакцией А.В.Крутских, А.В.Бирюкова «Инновационные направления современных международных отношений»[16].

Следует особо отметить труды коллектива Института экономических стратегий (ИНЭС)[17] на базе методологии «Стратегической матрицы»[18].

Начиная с 2007 г., метод «Стратегической матрицы» был модифицирован для решения прикладной задачи оценки и прогноза изменения интегральных показателей мощи государств[19]. Читатель сможет познакомиться в четвертой главе данной книги с современными информационно-аналитическими комплексами ИНЭС по поддержке принятия решений в сфере международных отношений.

Чрезвычайно интересен инновационный проект «Политический атлас современности, предпринятый МГИМО(У) МИД России в 2005-2007 гг. совместно с Институтом общественного проектирования при поддержке журнала «Эксперт».

Цель проекта - осуществить комплексный сравнительный анализ 192 стран мира, разработать их многомерную классификацию. В нем, наряду с методами политической компаративистики, исполь-

---

[14] Международная безопасность России в условиях глобализации / Под общ.ред. В.А.Михайлова, В.С.Буянова. - М.: РАГС, 2007

[15] Военная сила в международных отношениях: учебное пособие / Под общ.ред. проф.В.И.Анненкова. – М.: Восток-Запад, 2009

[16] Инновационные направления современных международных отношений: Учеб.пособие / А.В.Бирюков, Е.С.Зиновьева, А.В.Крутских и др.; Под ред. А.В.Крутских и А.В.Бирюкова. - М.: Аспект Пресс, 2010.

[17] А.И.Агеев, Б.В.Куроедов, О.В.Сандаров Методология стратегической матрицы. М.: ИНЭС, 2004.

Б.Н.Кузык, А.И.Агеев, О.В.Доброчеев, Б.В.Куроедов, Б.А.Мясоедов. Россия в пространстве и времени. М.: ИНЭС, 2004

[18] А.И.Агеев, Б.В.Куроедов. Стратегическая матрица Украины. М.: ИНЭС, 2005

А.И.Агеев, С.П.Головаченко, Б.В. Куроедов. Стратегическая матрица Беларуси. М.: ИНЭС, 2005

А.И.Агеев, А.Байшуаков, Б.В.Куроедов. Стратегическая матрица Казахстана. 2-е издание, дополненное и переработанное. М.: ИНЭС, 2006

А.И.Агеев, А.Г.Апостолов, Б.В.Куроедов. Стратегическая матрица Болгарии от древнейших времен до середины XXI века. М.: ИНЭС, 2006

Агеев А.И., Куроедов Б.В. Особенности применения методологии «Стратегической матрицы» при прогнозировании перспектив развития государств (на примере России и Китая). 2-е издание. М.: ИНЭС, 2008

[19] Глобальный рейтинг интегральной мощи 50 ведущих стран мира. Доклад к обсуждению. М.: МЛСУ, МАИБ, ИНЭС, 2007

Глобальный рейтинг интегральной мощи 100 ведущих стран мира. Доклад к обсуждению. М.: МЛСУ, МАИБ, ИНЭС, 2008

зуются различные методы многомерного статистического анализа (регрессионный, дискриминантный, кластерный, метод главных компонент и др.)[20].

В 2010 г. вышел первый том Энциклопедического справочника «Политические системы современных государств», посвященный государствам Европы, готовятся в печать следующие три тома - «Америка. Австралия и Океания», «Азия» и «Африка»,

По мере публикации печатной и электронной версии справочника планируется его обновление в открытом доступе. Кроме того, предполагается и институциональное развитие проекта «Политический атлас современности», который способен стать одним из системообразующих центров всей отечественной школы международных исследований[21].

Вышеназванные труды реферативно использованы в данной работе, которая, естественно, опирается на Стратегию национальной безопасности до 2020 года, Концепцию внешней политики, Военную доктрину и другие основополагающие документы Российской Федерации.

Особое место занимают выступления Д.А.Медведева[22] по международной проблематике, в т.ч. на совещании с российскими послами и постоянными представителями при международных организациях 12 июля 2010 г. Тема совещания - «Российская дипломатия: защита национальных интересов и содействие комплексной модернизации страны». В выступлении Президент России отметил, что в настоящее время происходит смена парадигмы международных связей и это дает уникальный шанс максимально эффективно использовать внешнеполитический инструментарий для модернизации страны[23].

В книге использованы материалы по изучаемой проблематике ООН, ЮНЕСКО, НАТО, G20, G8, ЕС, ОБСЕ, ОЭСР, БРИК, ШОС, АТЭС, СБЕР, ЧЭС и ряда других международных и региональных организаций, а также внешнеполитических ведомств ведущих государств мира и авторитетных отечественных и зарубежных организаций и экспертов.

[20] http://www.worldpolities.org
[21] http://www.worldpolities.org
[22] http://www.kremlin.ru/transcripts/5979
[23] http://news.kremlin.ru/transcripts/8325/print

Глава 1
К МАТРИЦЕ ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ: ОСНОВНЫЕ ЭТАПЫ, ТРЕНДЫ И ПОНЯТИЯ

Мы избегнем половины разногласий,
если сойдемся в определениях.

ДЕКАРТ

1.1. Коллективная безопасность

За 5000 лет на планете произошло около 14 тысяч войн, которые унесли жизни около 5 млрд.чел. При этом за последние 3400 лет цивилизация имела всего лишь 250 лет всеобщего мира[24].

Источник: Кафедра исследований проблем мира и конфликтов Уппсальского университета; и Международный институт мира в Осло.

Не без влияния данного фактора термин «безопасность» длительное время замещался понятиями «мир» и «война». При этом последняя рассматривалась как зло, но неизбежное. Термин «безопасность» вошел в документы **Лиги Наций** после колоссальных потерь Первой мировой войны. Тогда же в лексикон вошло понятие **коллективная безопасность**.

В годы холодной войны тема «безопасность» стала особой, ибо мобилизовывала военно-экономические, идеологические и иные ре-

[24] См.Пикте Ж. Развитие и принципы международного гуманитарного права. М. 1994

сурсы биполярного мира. Позднее понятие «безопасность» вошло в лексикон НАТО и стало ключевым объектом исследований политологов.

В СССР сохранялись термины «война» и «мир», хотя, по сути, речь шла о понятии «безопасность», а политбюро ЦК КПСС дефакто выполняло функции совета национальной безопасности. В ходе подготовки и проведения Совещания по безопасности и сотрудничеству в Европе (Хельсинки, 1975 г.) это понятие вошло и в лексику советских руководителей, хотя, как и иные «западные термины», первоначально оно подвергалось критике[25].

1.2. Всеобщая безопасность

В 1982 г. в докладе комиссии У.Пальме было введено понятие **«всеобщая безопасность»**, которое приобрело в нашей стране особую популярность в годы перестройки в рамках концепции нового политического мышления. Институциональную основу термина составляют не только и не столько военно-политические альянсы (как в случае с коллективной безопасностью), сколько глобальные организации типа ООН.

В эвристическом плане понятие «всеобщая безопасность» относительно «коллективной безопасности», несомненно, - шаг вперед. Однако оно страдало рядом недостатков: расплывчатость определения международной безопасности (понятие «безопасность» стало синонимом общественного блага), отсутствие иерархии приоритетов, слабое институциональное подкрепление и связанная с этим трудность практического воплощения в ходе строительства региональных или глобальных систем безопасности.

1.3. Кооперационная безопасность

Концепция кооперационной[26] безопасности стала популярной в середине 1990-х гг.[27] По мнению ее сторонников, она воплотила в себе лучшие стороны двух предыдущих концепций: признает многомерный характер безопасности и устанавливает определенную

[25] См. Петровский В.Ф. Доктрина «национальной безопасности» в глобальной стратегии США. М., 1980

[26] Некоторыми исследователями используется также термин «кооперативная»

[27] См. Цыганков П.А. Безопасность: кооперативная или корпоративная? (Критический анализ международно-политической концепции) // Политические исследования. № 3. 2000

иерархию приоритетов в решении первоочередных задач. При этом предпочтение отдается политическим средствам решения конфликтов, однако не исключается и применения военной силы, в т.ч. как инструмента превентивной дипломатии и миротворчества[28]. Признавая государство-нацию в качестве основного субъекта международных отношений, эта концепция, тем не менее, большое внимание уделяет использованию потенциала международных и транснациональных организаций.

В то же время модель кооперационной безопасности содержит ряд нерешенных проблем. Не до конца ясны ее конкретные параметры: какие институты должны стать ядром новой системы международной безопасности, какова природа силы и границы ее использования в современных условиях, каковы перспективы национального суверенитета, какова судьба существующих военно-политических альянсов, как предотвратить возрождение блоковой политики и скатывание нынешней системы международных отношений к хаосу и т.д.? Кроме того, вызывают опасение и попытки некоторых государств и коалиций интерпретировать понятие «кооперационной безопасности» в выгодном для себя смысле и построить не равноправную, а иерархичную систему международных отношений.

После трагедии 11 сентября 2001 г., приведшей к созданию широкой международной антитеррористической коалиции (с активным участием России), появились признаки того, что российские элиты проявляют склонность к кооперационной модели. Несмотря на временное охлаждение отношений между Россией и США из-за иракской войны, сотрудничество по таким глобальным вопросам, как нераспространение ОМУ, сокращение военных потенциалов и разоружение, борьба с международным терроризмом, оргпреступностью, наркобизнесом, по-прежнему продолжается, а по некоторым направлениям, набирает обороты.

1.4. Матрица глобальной и национальной безопасности: вызовы и парадигмы 21 века

Новые вызовы и угрозы, в т.ч. межцивилизационные коллизии, международный терроризм, мировой финансово-экономический кризис, энергетическая и информационная безопасность, природогенные, техногенные и социогенные катастрофы, климатические катаклизмы, пандемии и т.д. остро поставили вопрос о необходимо-

[28] См.Зимин П. Вызов глобализации // Русский журнал, 2002

сти обеспечения качественно **новой парадигмы безопасности - глобальной**. При этом проблематику международной безопасности, включая военно-политическую составляющую, ряд экспертов относит к традиционным форматам внешнеполитической деятельности.

Позицию России по данной проблеме предельно ясно сформулировал Д.А.Медведев в своем выступлении на международной конференции «Современное государство и глобальная безопасность» (Ярославль, 14 сентября 2009 г.): «Ответственность государств перед гражданами и друг перед другом, их эффективность в обеспечении общественной и глобальной безопасности - вот что нам необходимо»[29]. В итогах 2010 г. (24 декабря 2010 г.) Президент России подчеркнул: «Безопасность нами понимается не только как внутренняя ситуация, хотя это, безусловно, очень важно, но и как глобальная безопасность» [30].

Современное видение военно-политических аспектов проблемы, а также внешнеполитическую философскую базу, на которую опираются все российские усилия в сфере безопасности, дал С.В.Лавров: «…речь вовсе не идет о коренном сломе устоявшихся систем безопасности. Подразумевается лишь модернизация и укрепление их элементов, выработка в дополнение к ним новых, и главное - придание такому нормотворчеству общесистемного характера. Это позволило бы создать единую «правовую платформу» системы гарантий в военно-политической сфере, своего рода **матрицу глобальной безопасности**»[31].

1.4.1. Концепция «столкновения цивилизаций»

В проблеме глобальной безопасности особое внимание занимает концепция **«столкновения цивилизаций»** С.Хантингтона. Ее суть в том, что на смену конфликтов между государствами-нациями, или идеологиями в 20 веке, приходят конфликты между 7-8 цивилизациями, т.е.:

- западной,
- конфуцианской,
- японской,
- исламской,

[29] http://www.kremlin.ru/transcripts/5469
[30] http://www.kremlin.ru/transcripts/9888
[31] «Новый Договор о СНВ в матрице глобальной безопасности. Политическое измерение»/ «Международная жизнь» № 7, июль, 2010

- индуистской,
- славянско-православной,
- латиноамериканской
- и (возможно) африканской.

Большинство экспертов, соглашаясь с наличием цивилизационных различий и коллизий на бытовом уровне, тем не менее, считают, что они достаточно условны. В этом контексте трудно согласиться с позицией Г.Юрьева, изложенной в гайд-парке в триптихе «Глобальный конфликт цивилизаций» [32]. Так, в ходе войны в Ираке в 1991 г. большинство арабских государств присоединилось к антииракской коалиции (а в нее входили государства различных цивилизаций).

Нынешняя угроза исламского терроризма - это столкновение лишь части исламской цивилизации с иными цивилизациями. Кроме того, **существующие военные союзы между США и Японией, Россией и странами Центральной Азии, а также иные в большей части дезавуируют прогноз С.Хантингтона и его сторонников.**

1.4.2. Национальная и глобальная безопасность: позиция США

В США Закон «О национальной безопасности» был принят в 1947 г. Четкого определения понятия «национальная безопасность» в нем не дано. Ряд экспертов полагают, что это объясняется его проработанностью в политологических исследованиях[33].

Закон базируется на опыте ведения Второй мировой войны, а также особенностей обеспечения безопасности в конкретных исторических условиях. В соответствии с Законом были созданы минобороны, ЦРУ, управление по мобилизации материальных и людских ресурсов, а также Совет национальной безопасности (СНБ). Позднее некоторые институты были реформированы, появились новые, но в целом система сохранила свою преемственность.

Согласно Конституции США, президент наделен основными полномочиями в реализации политики и принятии концептуальных документов по национальной безопасности. При президенте США функционирует СНБ – главный координационный инструмент в сфере внешней, внутренней и оборонной политики. В СНБ входят

[32] http://gidepark.ru/user/2091965604/article/135171
[33] См. И.В.Макаренкова. Современные зарубежные концепции национальной безопасности http://www.council.gov.ru/inf_sl/bulletin/item/364/index.html

по должности: вице-президент, госсекретарь, министр обороны, начальник управления мобилизации. На заседаниях СНБ присутствуют также постоянные советники - директор ЦРУ и председатель Объединенного комитета начальников штабов, помощник (советник) президента по национальной безопасности, а также министры финансов, юстиции и др.

В штате Белого дома СНБ на уровне руководства занимаются: помощник (советник) президента по нацбезопасности, исполнительный секретарь СНБ (ему подчинены четыре члена директората СНБ, имеющие статус помощников министра и назначаемые президентом) и директор группы «ситуационного анализа». **Данная группа использует Ситуационный центр, оснащенный новейшими ИКТ: аналитическими, экспертно-моделирующими и телекоммуникационными для проблемного мониторинга и подготовки вариантов кризисного реагирования для доклада президенту** (подробнее см. в гл. 3).

Важнейшие доктринальные документы, рассматриваемые в СНБ, - это Стратегия национальной безопасности США (она излагается в посланиях президента Конгрессу) и Национальная военная стратегия (разрабатывается Объединенным комитетом начальников штабов США каждые 2-3 года).

Национальная военная стратегия - это составная часть Стратегии нацбезопасности США. Документ включает строительство и использование ВС и является американской военной доктриной:

- трактовку предназначения ВС США в современных условиях;
- обобщенный анализ военно-стратегической обстановки в мире;
- формулировку военных целей национальной безопасности США;
- пути достижения военных целей (элементы стратегии, стратегические концепции строительства и боевого применения вооруженных сил США);
- состав сил, требуемый для достижения целей национальной безопасности при приемлемой степени риска.

Законодательная ветвь власти в США непосредственно не участвует в механизме выработки, принятия и реализации внешнеполитических решений и ее представители не входят в СНБ. Однако Конгресс способен влиять на этот процесс через бюджетную политику, организацию различных слушаний «в порядке надзора» с участием представителей исполнительной власти, через запросы в органы исполнительной власти, при ратификации международных

соглашений и договоров, при утверждении назначений на должности послов и других должностных лиц внешнеполитического ведомства и т.д.

Решения президента США в сфере национальной безопасности можно достаточно условно разделить на следующие категории:

1. Решения, принимаемые в чрезвычайных условиях и требующие незамедлительных действий. Это решения о применении стратегических ядерных сил в случае внезапного ядерного удара по США, а также использования вооруженных сил при нападении на США или их объекты за рубежом, равно как в случае стихийных бедствий, массовых беспорядков и т.д.

2. Формирование внешнеполитического курса и политики в сфере безопасности США с учетом изменения ситуации в стране и во всем мире. Данные решения отражаются в ежегодном докладе президента Конгрессу «Стратегия национальной безопасности США».

3. Военно-политические и экономические решения по внутренним проблемам, строительству и направлению развития вооруженных сил, военно-промышленного комплекса и т.д.

4. Текущие решения по внутриполитическим или внешнеполитическим проблемам, которые принимаются оперативно, с учетом складывающейся в данный момент политической, военной и экономической ситуации.

1.4.2.1. Концепция конкурирующих стратегий

В последние годы в США все шире практикуется **концепция конкурирующих стратегий**. Она предусматривает разработку альтернативных решений проблем, их детальную экспертную проработку и обоснование. При этом активно используются не только разведывательные или иные ведомства, обладающие мощными информационно-аналитическими возможностями, но и независимые (или частично независимые) институты («мозговые тресты»).

В мае 2010 г. администрация Б.Обамы утвердила новую Стратегию национальной безопасности США. В основе документа лежит прагматичное понимание сущности стратегии США в мире. Некоторые аспекты новой Стратегии кардинально отличаются от предыдущего документа.

В нем отмечается вовлеченность США в войну, а также продолжающийся экономический кризис, дан перечень угроз национальной безопасности США, в который наряду с распространением ОМУ и ядерного вооружения, терроризмом и увеличением кибер-

преступлений, входят иммиграция и энергетическая составляющая. **Новеллами стали включение проблем изменения климата и зависимости США от природного топлива как фундаментальных проблем национальной безопасности**.

Впервые в Стратегии на правах одной из центральных угроз США поставлен «домашний» терроризм, т.е. вопрос внутренней безопасности и ее обеспечения властями и специальными службами.

1.4.3. Особенности концепций национальной безопасности европейских государств

1.4.3.1. Великобритания

23 ноября 2010 г. в Главном управлении международного военного сотрудничества Минобороны России прошел брифинг британского атташе по вопросам обороны бригадного генерала авиации М.Макгеона и военно-морского атташе капитана 1 ранга С.Эйри по основным положениям Стратегического обзора политики Великобритании по вопросам обороны и безопасности, который был обнародован в Лондоне 19 октября 2010 г.[34]

Появление обновленной Стратегии национальной обороны и безопасности Великобритании ожидалось (документ не пересматривался с 1988 года).

Правительство Великобритании впервые приняло решение в отношении обороны, безопасности, разведки, устойчивости, развития и внешнеполитических возможностей комплексно:

- был принят ряд жестких мер, учитывая необходимость в сокращении дефицита национального бюджета;
- в целом, Стратегия национальной обороны и безопасности обеспечит оборону Великобритании на современном уровне: Вооруженные Силы и вооружение, адекватные вызовам 21-го века; сильные службы безопасности и разведки; эффективные внешнеполитические и внешнеэкономические службы;
- дополнительные ресурсы будут направляться на работу по первоочередным рискам: разработка новой гибкой госпрограммы кибербезопасности (650 млн.ф.ст.) и обеспечение ресурсами мероприятий по борьбе с терроризмом в прежнем объеме;

[34] http://ukinrussia.fco.gov.uk/ru/news/?view=News&id=378756682

- больше ресурсов будет направлено на предотвращение и борьбу с угрозами в очагах их возникновения. Бюджет международного развития будет максимально нацелен на решение задач национальной безопасности в соответствии с Государственным регламентом содействия. Объем финансирования в «горячих точках» возрастет с двух до четырех млрд.ф.ст. к 2014-2015 финансовому году;
- увеличится объем госфонда предотвращения конфликтов. Фонд финансируется мининдел, минобороны и международного развития;
- ядерная ракетная система сдерживания «Трайдент» останется на вооружении. Пересмотр программы «Трайдент» позволит сэкономить 3 млрд.ф.ст. в ближайшие десять лет;
- будет поддерживаться оборонный потенциал во всем диапазоне на уровне, позволяющем развертывать группировки войск за рубежом и защищать свои национальные интересы;
- сохранятся расходы на оборону на принятом в НАТО уровне 2% от ВВП, что позволит ей удерживать 4-е место в мире по военным расходам. Участие в военных операциях в Афганистане продолжится;
- сильные союзнические и партнерские отношения являются краеугольной составляющей британской Стратегии национальной безопасности и обороны. Великобритания укрепит исключительные отношения с США в области безопасности и обороны, упрочит партнерство с Францией и будет наращивать двусторонние отношения в области обороны и безопасности с рядом партнеров;
- будет оказываться поддержка многосторонним организациям, являющимся ключевыми для ее национальной безопасности и повышения их эффективности;
- совет национальной безопасности будет контролировать реализацию Стратегии, а ведущие министры будут наделены обязанностями по координации работ по приоритетным направлениям внутри Правительства;
- деятельность в области обороны и безопасности за рубежом также будет более скоординированной, где Министерство иностранных дел будет ведущим, в т.ч. путем тесного взаимодействия с другими ведомствами и реализации совместных стратегий.

1.4.3.2. Франция

В июне 2008 г. был представлена Белая книга по обороне и национальной безопасности Франции (заменила документ 1994 г.).

В ней определены следующие угрозы безопасности Франции, связанные с глобализацией:

- терроризм;
- распространение оружия массового поражения;
- атаки на космические и информационные системы;
- финансово-политические кризисы;
- конкуренция за доступ к водным, энергетическим ресурсам, источникам сырья;
- ухудшение качества окружающей среды, пандемии, неконтролируемая миграция.

Среди приоритетов национальной безопасности Франции выделяются:

- утверждение независимого статуса за счет обладания ядерным потенциалом и значительной военной мощью;
- участие в формировании политики НАТО;
- дальнейшее укрепление Евросоюза через валютный союз и франко-германское взаимодействие.

Политика России в отношении с соседями названа «важным фактором», влияющим на безопасность на континенте и в мире. При этом в документе критикуется политическое и энергетическое давление России на некоторые страны бывшего СССР.

Президент Франции Н.Саркози в качестве важнейшего внешнеполитического приоритета также определил укрепление двусторонних отношений с США.

Согласно новой стратегии, создан единый Совет обороны и национальной безопасности. Управление безопасности территории (DST) преобразовано в Центральное управление внутренней разведки (DCRI), основной задачей которого объявлена борьба с терроризмом (международным, европейским, внутрифранцузским), в т.ч. путем агентурной работы.

В документе Франция объявила зоной своих национальных интересов Западную Африку и Сахару. Это мотивируется общностью культуры, истории, языка и взаимных экономических интересов африканских государств и Франции, необходимостью усилить общую безопасность в формате партнерских отношений. При этом предполагается сокращение военных баз в Африке и численности дислоцированных за рубежом войск с 50 до 30 тыс. человек.

Франция выступает за создание «европейской обороны», «европейской оборонительной доктрины» с перспективой формирования единой «европейской армии». В качестве главного аргумента выдвигается тезис о невозможности в национальном формате противостоять новым вызовам и угрозам.

Эти идеи находят поддержку далеко не во всех государствах Евросоюза. Оппонентом французской инициативы выступила Великобритания, которая высказалась против дублирования командных структур НАТО. **Однако США подталкивают британских союзников к достижению договоренности с Н.Саркози по поводу общеевропейской системы безопасности.**

1.4.3.3. Германия

В Германии понимание проблем национальной безопасности тесно увязывается с необходимостью изменения задач бундесвера.

В октябре 2006 г. правительство ФРГ приняло «Белую книгу по вопросам политики безопасности Германии и будущего бундесвера» (заменила документ 1994 г.).

Согласно официальной позиции военно-политического руководства ФРГ, угрозы и риски современной Германии приобретают комплексный характер и могут возникнуть в любое время в любой точке мира. При этом руководство ФРГ считает, что ни одно государство в современных условиях не может собственными силами обеспечить для себя мир, безопасность и благополучие.

Исходя из этого, стратегия национальной безопасности ФРГ предусматривает тесное взаимодействие с союзниками и партнерами, использование комплексного подхода к обеспечению всех аспектов безопасности (внутренних и внешних, политических, экономических, экологических, социальных и др.), а также реализацию принципа превентивности выявления кризисов и заблаговременное предотвращение их опасных последствий. **Важным в доктринальных документах ФРГ является тезис о стирании границ между внутренней и внешней безопасностью**.

Руководство Германии рассматривает вооруженные силы как универсальный инструмент госполитики, направленной на гарантированное обеспечение национальной безопасности и предназначенной для парирования любых угроз, с какими только может столкнуться страна уже в ближайшем будущем.

1.4.4. Концепция национальной безопасности Китая

С учетом того, что Китай способен превзойти США в военной сфере, особый интерес представляет современная концепция национальной безопасности КНР.

Ее положения излагаются в программных документах съездов компартии, постановлениях пленумов и Центральной военной комиссии ЦК КПК, а также в документах Центрального военного совета и Госсовета КНР. Основные позиции по этой теме в их официальной трактовке представляются в Белой книге «Национальная оборона Китайской Народной Республики» (с 1998 г. опубликовано 6 книг, последняя - в январе 2009 г.).

Документ был выпущен на китайском и английском языках и приурочен к инаугурации президента США Б.Обамы. КНР выразила надежду, что США воспользуются возможностью улучшить военные отношения с Китаем. Одновременно, Китай назвал одним из факторов нестабильности усиление присутствия США в АТР и оставил за собой право использовать ядерное оружие в ответ на ядерную атаку.

Основным принципом СНБ КНР, является опора на собственные силы, главными компонентами которых считаются экономика, наука и техника, внутриполитическая стабильность и военная мощь. В качестве главного условия и основы успешного экономического развития называется «создание мирного окружения» (военно-политический аспект безопасности) и «экономическая интеграция с соседями по региону» (экономический аспект).

Одной из важных задач в области обеспечения национальной безопасности является предотвращение локальной войны в регионе. Главным средством этого являются вооруженные силы, которые должны повышать свою маневренность, огневую мощь и гибкость системы управления, а также добиваться более полного использования научных достижений в своей деятельности. В этом контексте не исключается и военная форма экспансии в отношении Тайваня.

В новой «Белой книге» отмечается, что существуют шансы избежать полномасштабной войны глобального характера в сравнительно долгосрочной перспективе, поскольку возрастает число благоприятных факторов для защиты мира.

Резюмируя, следует отметить, что концептуальные документы ведущих стран мира по проблеме обеспечения национальной безопасности в глобальном контексте зачастую лишь маскируют истинные цели государств риторикой, а декларируемые постулаты нередко расходятся с практическими шагами на международной арене.

1.4.5. Базовые положения концепций национальной безопасности стран ближнего зарубежья

1.4.5.1. Белоруссия

9 ноября 2010 г. президент Белоруссии А.Г.Лукашенко своим указом № 575 утвердил Концепцию национальной безопасности страны. Документ определяет место и роль Белоруссии в условиях глобализации международных отношений[35].

Сохранена преемственность с ранее действовавшими концепциями 1995 и 2001 годов. Одновременно, развит ряд важнейших направлений обеспечения национальной безопасности, использованы принципиально новые подходы.

Уточнены и расширены ключевые понятия. Основные сферы национальной безопасности дополнены научно-технологической и демографической сферами. Определены роль и место Белоруссии в условиях глобализации международных отношений. Впервые изложены основные национальные интересы, представляющие собой совокупность потребностей государства по реализации сбалансированных интересов личности, общества и государства. Существенно расширена характеристика текущего состояния национальной безопасности.

Если в предыдущей Концепции национальной безопасности Белоруссии речь шла исключительно об основных факторах, создающих угрозы национальной безопасности, то в новой они существенно расширены и уточнены. Разделены понятия «угрозы» и «источники угроз», как внутренних, так и внешних, приведен их перечень.

Реализован новый подход применительно к построению системы обеспечения национальной безопасности. Выделены сущность, принципы и цель обеспечения национальной безопасности, основные задачи, которые необходимо решать для ее достижения, главные направления этой деятельности. На основании общих положений определен состав системы обеспечения национальной безопасности (субъекты и силы), их основные полномочия.

Предусмотрено создание комплексной системы стратегического планирования. В качестве основы ее документов обозначены настоящая концепция и программы социально-экономического развития страны. Впервые вводится система индика-

[35] http://www.belta.by/ru/all_news/president/Kontseptsija-natsionalnoj-bezopasnosti-utverzhdena-v-Belarusi_i_531114.html

торов состояния национальной безопасности, характеризующих текущий уровень и динамику изменения состояния национальной безопасности в различных сферах.

В целом новая Концепция национальной безопасности Белоруссии выступает концептуальной и методологической основой для консолидации усилий и повышения эффективности деятельности госорганов и иных организаций, граждан страны по обеспечению национальной безопасности, защите ее национальных интересов.

Военная доктрина Белоруссии, принятая в 2002 г., исходит из того, что ни одна другая страна в настоящее время не является для республики потенциальным противником. Внешними угрозами Белоруссия признает, например, вмешательство в свои внутренние дела, расширение военных блоков и союзов в ущерб военной безопасности республики, а также «целенаправленное, противоречащее интересам Республики Беларусь и ее союзников информационное (информационно-психологическое) воздействие с использованием современных информационных технологий». Помимо этого, в документе подчеркивается, что Белоруссия занимается формированием единого оборонного пространства с Россией.

1.4.5.2. Украина

В военной доктрине Украины (2004 г.) отмечается, что ни одна страна не является ее противником, но потенциальным противником станет государство, последовательная недружелюбная политика которого будет угрожать военной безопасности страны. Внешними угрозами Украина считает в т.ч. возможность втягивания в региональные войны, военно-политическую нестабильность и конфликты в соседних государствах и незавершенность договорно-правового оформления своей государственной границы. Одной из базовых концепций обеспечения военной безопасности указано «предотвращение возможной вооруженной агрессии путем ее военно-силового сдерживания, в частности, путем создания угрозы причинения потенциальному агрессору вреда, неадекватного ожидаемому». В документе также неоднократно упоминается намерение Украины присоединиться к НАТО.

С избранием президентом Украины В.Януковича в развитии системы национальной безопасности можно выделить три ключевых блока проблем[36]:

[36] http://www.politika.org.ua/?p=1411

- принципов, приоритетов и «реалитетов» реформирования сектора безопасности;
- развитие механизмов демократического контроля над его деятельностью;
- оптимизации отношений между ключевыми субъектами сектора безопасности (начиная с отношений Президента, Кабинета Министров и СНБО Украины и заканчивая отношениями МВД и СБУ, ГУР МО и СВР и т.п.).

При этом каждый блок проблем требует соответствующего системного анализа.

1.4.5.3. Грузия

В 2005 г. Грузия опубликовала «Национальную военную стратегию». Ее разработка была предусмотрена программой индивидуального партнерства Грузии с НАТО. В документе, над которым работали специалисты грузинского Генштаба, члены парламента и неправительственных организаций, а также зарубежные эксперты, одной из главных угроз названо российское военное присутствие на базах в Грузии (последняя из них была выведена в 2007 г.), наличие неконтролируемых территорий и присутствие в них российских контингентов и территориальная целостность страны. В Стратегии указано, что грузинская армия должна быть трансформирована и перевооружена по стандартам НАТО в 2010 г. Вероятные противники Грузии в документе не упоминаются, союзниками названы США и другие страны НАТО.

В первую годовщину агрессии Грузии против Южной Осетии и миротворцев России в августе 2009 г. власти Грузии объявили, что пересмотрят национальную военную доктрину и концепцию безопасности страны. Независимо от своих отношений с НАТО и США, руководство Грузии пришло к выводу, что в интересах национальной безопасности и выживания ей необходима собственная оборона и способности сдерживания.

Глава 2
ОБЗОР БАЗОВЫХ ПОДХОДОВ К АНАЛИЗУ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ И КОНФЛИКТОВ

От бокала шампанского настроение
поднимается, разыгрывается
фантазия и чувство юмора, но от
целой бутылки кружится голова.
Примерно так же действует и война!
Чтобы по-настоящему
почувствовать вкус и того, и другого,
лучше всего заняться дегустацией…

УИНСТОН ЧЕРЧИЛЛЬ,
«Вторая мировая война»

2.1. Исторический и научный подходы

Теоретически существует несколько подходов к анализу международных отношений. Американский исследователь П.Бэкман классифицирует все подходы на исторические и научные. Однако на практике чаще всего используется их комбинация.

Исторический подход основывается на изучении исторических артефактов, событий, документов, летописей, мемуаров и т.д. При этом особое внимание уделяется расследованию и учету обстоятельств, окружающей исторической среды, в которой имели место события.

Принципиальное отличие данного подхода от научного - это тезис об уникальности каждого исторического события и о невозможности его вычленения из исторического контекста. **Недостатком этого подхода является невозможность выявления закономерностей событий и структуры международных процессов, а также прогнозирования их развития**.

По этой причине исторический подход используется, как правило, на начальном этапе других подходов для того, чтобы получить наиболее полные исходные данные для анализа конфликта. Одним из основателей историко-социологического подхода является французский социолог Р.Арон[37].

[37] Aron K. Paix et Guerre entre les nations. Paris, 1984. P. 103

Научный подход классифицирует события, сходные по природе, типологии и причинам, в слабой увязке с историческим контекстом. Данный подход позволяет выявлять закономерности международных процессов и прогнозировать их развитие. Вместе с тем, он чреват абстрагированием от реальности, искажением действительности и, как следствие, невозможностью объективного анализа исторического процесса.

В научном подходе выделяют следующие четыре вида: **геополитический, бихейвиористский, интерактивный и системный**.

2.1.1. Геополитический подход

В геополитическом подходе основное внимание уделяется анализу внутренних и внешних факторов существования системы или условию протекания процесса. Т.е. география и пространство выступают как главные факторы развития цивилизации. Зависимость человека от пространства - основной тезис геополитики. Главным законом геополитики является утверждение фундаментального дуализма - в противостоянии «теллурократии» (сухопутного могущества) и «талассократии» (морского могущества). Основатель геополитики англичанин Х.Маккиндер в начале XX столетия не только поделил весь мир на две суперцивилизации - морскую и континентальную, не только заложил в их отношения семена вечной вражды, но и предложил формулу мирового господства для англосаксов. **Возведя Россию в ранг сердцевины земного шара (Хартленда), Маккиндер сделал вывод о том, что без контроля над Хартлендом (Россией) мировое господство англосаксов невозможно**.[38]

«Тот, кто контролирует Восточную Европу, доминирует над heartland'ом;

тот, кто доминирует над heartland'ом, доминирует над Мировым Островом;

тот, кто доминирует над Мировым Островом, доминирует над миром»[39].

Многие аналитики используют данный закон для объяснения причин глобальных конфликтов.

Другой составляющей геополитического подхода являются внутренние аспекты объекта исследования: политическая система

[38] См. http://www.mstu.ru/forum/index.php?topic=21092.0
[39] Mackinder H. Democratic ideals and reality, New York, 1919. P. 34.

государства, социально-экономический, военный, научно-технический, информационный потенциал, этноконфессиональный состав и т.д.

2.1.2. Бихейвиористский подход

В бихейвиористском подходе анализируется две составляющие: лица, принимающие решения, и сам политический процесс.

Сначала формулируется проблема, затем вырабатываются цели, которые необходимы для разрешения проблемы (исходя из национальных интересов). Далее рассматриваются варианты действий для достижения цели, затем выбирается и реализуется наиболее оптимальный из них.

Искусство принятия решения, иными словами управления внешнеполитическим процессом, состоит также и в умении лицами, принимающими решения, доказывать его предпочтительность как оптимального. **В реальных ситуациях не бывает решений, принятых исключительно на основе рационального подхода или исходя лишь из политической необходимости. Это всегда синтез обеих составляющих.**

2.1.3. Интерактивный подход

Интерактивный подход рассматривает взаимодействие на уровне государств и иных субъектом межгосударственных отношений. Его суть можно изобразить в виде следующей схемы.

В данном подходе ставятся три вопроса:

1. Каким образом государства взаимодействуют между собой?
2. Почему они выбирают тот или иной путь взаимодействия?
3. Каковы будут результаты от выбранного взаимодействия?

В качестве ответа на вопросы используются следующие три метода, **теория игр, теория торга и моделирование**.

2.1.3.1. Теория игр

С помощью теории игр можно построить математическую модель поведения игроков, в т.ч. в международном конфликте. Условия построения модели:

- поведение игроков рационально, то есть они стремятся увеличить свой выигрыш или минимизировать проигрыш;
- возможности выбора ограничены и определены;
- выбор одного игрока зависит от выбора другого;
- выбор игрока обусловлен «ценой», которую ему придется заплатить при любом исходе.

Модель можно представить следующим образом:

		Государство А	
		Стратегия 1	**Стратегия 2**
Государство Б	**Стратегия 1**	**Исход 1**	**Исход 2**
	Стратегия 2	**Исход 3**	**Исход 4**

Игроки выбирают тактику, исходя из того, сколько они рискуют проиграть или выиграть (стоимости исходов 1, 2, 3, 4) и с учетом тактики оппонента.

2.1.3.2. Теория торга

По теории торга (по В.Зартману)[40] государства, которые вовлечены в конфликт, признают, что существует его взаимоприемлемое решение. При этом одна из сторон корректирует свои цели или ей удается убедить другую сторону принять ее предложения, или изменить свои условия.

Данный метод исключает решение конфликта силовым или юридическим путем. Основой метода является постоянное взаимодействие сторон. При этом уступчивость одной стороны способна побудить другую сторону твердо стоять на своих требованиях. При неуступчивости обеих сторон достижение компромисса и договора маловероятно. **Данный подход эффективен для анализа поведения сторон в конфликте, когда они готовы урегулировать разногласия путем переговоров.**

[40] Zartman I William. Introduction in the 50% Solution, ed. I.W. Zartman, Garden City, 1976. P. 7-18

2.1.3.3. Моделирование

Моделирование рассматривает внешнеполитический процесс с точки зрения методов и способов взаимодействия, выбранных сторонами, и ищет причины их выбора.

Автор метода Л.Ричардсон на примере модели гонки вооружений двух государств исходит из предположения, что они оба имеют только мирные намерения. Вместе с тем, каждая из сторон подозревает другую в неискренности и полагает, что противоположная сторона может иметь враждебные намерения. Оба государства поддерживают свой потенциал на уровне, необходимом для защиты от возможной агрессии, но в глазах другой стороны вооружения нацелены на агрессию, что вызывает ответные шаги и так далее. Данная модель поведения государств описывается с помощью дифференциальных уравнений[41].

Ниже приведена классификационная таблица основных методов взаимодействия участников внешнеполитических процессов[42].

Конфликтные методы взаимодействия

Название метода	**Действия, характерные для метода взаимодействия**
Война	Применение военной силы
Кризис	Обмен угрозами применения военной силы или иных санкций
Гонка вооружений	Наращивание вооружения и его размещение
Проникновение	Непрямое воздействие и проникновение в социально-политическое устройство другого актора
Устрашение	Возможность государства нанести ответный удар после того, как оно подверглось атаке
Блоковое противостояние	Мобилизация членов блока для ответа на угрозу со стороны другого блока
Дипломатия	Обмен информацией и взаимодействие между государствами в своих интересах
Взаимодействие малых и больших стран	Совместные действия доминирующих и менее влиятельных стран и оказание взаимного давления в международных делах

[41] Richardson L. Arms and Insecurity: A Mathematical Study of the Causes and Origins of War / pacific Grove, Cal.: Box-wood Press, I960. P. 57-69

[42] См. Барановский Е.Г., Владиславлева Н.Н. Методы анализа международных конфликтов. – М.: Научная книга. 2002

Название метода	Действия, характерные для метода взаимодействия
Коллективные действия по решению проблем	Совместные действия акторов по решению проблем, представляющих угрозу для всего международного сообщества
Формирование союзов	Создание временных или постоянных институтов для выдвижения и защиты общих интересов
Интеграция	Частичный роспуск национальных институтов и органов и отказ от национальных интересов в пользу общих (наднациональных)

Следует подчеркнуть, что моделирование успешно применяется и в других подходах, в т.ч. в системном.

2.1.4. Основные понятия системного подхода

Системный подход интегрирует основные аспекты предыдущих подходов и широко используется в конфликтологии. Он стал внедряться в науку о международных отношениях в середине XX века, когда ЭВМ облегчили задачу моделирования, построения и расчета конкретных систем. Наиболее полно данный подход описал Д.Истон в книге «Системный анализ политической жизни»[43], который позволяет изучать систему международных отношений с учетом взаимосвязей ее элементов.

Базовое понятие: **система - это совокупность элементов, находящихся во взаимодействии друг с другом**.

Элемент - простейшая часть системы. В сложных системах элементом может являться и подсистема.

Связи - причинно-следственные зависимости между элементами системы.

Структура системы:

- соотношение элементов системы;
- способ организации элементов в систему;
- совокупность принуждений и ограничений, вытекающих из существования системы для ее элементов;
- внешняя среда - окружение системы;
- внутренняя среда - контекст.

[43] Easton D.A. Systems Analysis of Political Life. New York, 1965.

Функции системы - это ее реакция на воздействие извне, направленная на сохранение ее «устойчивости» (если коэффициент устойчивости S, то: $0 < S < 1$).

Системный подход широко используется для анализа конфликтов, хотя они многофакторны и трудно формализуемы.

2.1.5. Схема системного анализа внешнеполитического процесса

На базе системного подхода строится многоуровневая схема системного анализа международных явлений. Она состоит из определения:

- уровня изученности;
- внешней среды системы;
- типа системы;
- структуры системы (выделение элементов и связей);
- цели системы (в т.ч. установление целей ее элементов);
- списка альтернативных целей;
- альтернативных целей на основе затрат;
- критерия оценки для ранжирования альтернатив;
- чувствительности системы к альтернативным целям;

а также предусматривает:

- сбор информации;
- оценку достоверности информации;
- построение модели;
- оценку модели системы с помощью выбранного критерия (например, минимаксный критерий, т.е. при минимальных затратах - максимальный результат);
- прогнозирование реакции системы и изменение ее состояния при определенных внутренних и внешних воздействиях;
- возобновление процесса.

Под уровнями взаимосвязи государства и международных отношений, предлагается выделить следующие уровни:

- глобальный - насколько она влияет на мировую систему;
- региональный - культурно-национальные особенности взаимосвязи;
- национальный - национальные интересы государств;
- провинциальный - отношения между субъектами государства и государственностью;
- институциональный - разные ведомства один и тот же конфликт будут рассматривать по-разному;

- социальный;
- индивидуальный.

Данная схема используется при выявлении общей структуры международного конфликта и разработке алгоритма его моделирования.

2.1.6. Типы и способы урегулирования конфликтов

В конце XX в. Ф.Брайар и М.Р.Джалили выдвинули основанную на системном подходе концепцию детерминант внешней политики, идея которой состоит в том, что **внутренние и внешние факторы воздействуют на внешнюю политику государства, тесно взаимодействуя друг с другом**[44].

При этом они выделили следующие три группы международных конфликтов, которые отличаются по своей природе, мотивациям их участников и масштабам.

1. Классические межгосударственные конфликты, межгосударственные конфликты с тенденцией к интеграции, национально-освободительные войны и т.п.

2. Территориальные и не территориальные конфликты (могут иметь социально-экономические, идеологические мотивы или же вытекать из воли к могуществу).

3. Генерализованные (в них вовлечено большое количество государств), которые способны перерасти в мировые конфликты, а также региональные, субрегиональные и ограниченные (числом стран-участниц).

Имеются также иные классификации, критериями которых выступают причины и степень напряженности конфликтов, характер и формы их протекания, длительность и масштабы и т.д. Однако на практике каждая фаза конфликта развивается в рамках различных сфер функционирования субъектов конфликта: политической, военной, экономической, информационной, социальной и экологической.

Существуют три подхода к регулированию конфликтов:

- правовой (или нормативный);
- принудительно-переговорный;
- решение проблемы.

Первый способ требует консенсуса сторон. **Доминирующую роль в урегулировании конфликтов играет принудительно-пе-**

[44] Braillard Ph., Djalili M.-R. Les relations intemationales. Paris. 1990

реговорный способ или метод торга. Третий способ связан с достижением безопасности субъекта конфликта.

Наиболее часто используемым способом разрешения конфликта являются прямые и косвенные насильственные действия.

Практика свидетельствует о сохранении примата военного насилия в разрешении противоречий. В мирное время оно используется как угроза применения военной силы, что в политическом лексиконе принято называть «сдерживанием» или «устрашением». Последнее десятилетие дает немало примеров использования других насильственных способов политического, экономического, информационно-психологического и иного характера воздействия на субъекты конфликтов.

2.1.6.1. Типы переговоров

В предотвращении и урегулировании конфликта важную роль играют ненасильственные действия и, прежде всего, переговоры.

Существует три типа таких переговоров:

- переговоры - схватки;
- переговоры - торги;
- переговоры - игры.

Возрастание роли переговорной составляющей урегулирования конфликтов объясняется следующими факторами:

- международные переговоры активно воздействуют на дальнейшее уменьшение роли военного фактора;
- растет объем и количество переговоров. Их объектом становятся все новые области международного взаимодействия (экология, социально-политические процессы, научно-техническое сотрудничество и т.п.);
- возрастает переговорная роль международных организаций;
- в сферу переговоров вовлекаются эксперты без дипломатического опыта, но компетентные в области научно-технических, экономических, экологических и иных проблем для анализа новых сфер взаимодействия между государствами;
- возникает необходимость коренного пересмотра процесса управления переговорами:
  - выделения наиболее важных проблем для высшего руководства;
  - определение сферы компетенции рабочих уровней;
  - разработка системы делегирования ответственности;
  - повышения координирующей роли дипслужб и т.п.

2.2. Международный конфликт: определение, фазы развития

В теории международных отношений существует немало определений международного конфликта. Наиболее релевантным определением «конфликта» считается формулировка американского ученого Л.Козера: «**Конфликт - борьба за ценности и претензии на определенный статус, власть и ресурсы, борьба, в которой целями противников являются нейтрализация нанесение ущерба или уничтожение соперника»**[45].

В структуре международного конфликта выделяют три основные фазы:

- предконфликтное состояние;
- кризис;
- постконфликтное урегулирование.

В традиционных исследованиях модель международного конфликта рассматривается сначала как процесс, а затем как ситуация[46].

При этом конфликт рассматривается в качестве системы, состоящей из множества процессов международных отношений. Любой международный конфликт развивается в специфических и во многом неповторимых внутренних и внешних условиях и сам по себе уникален (к исключениям можно отнести алгоритм «цветных» революций с соответствующей международной реакцией).

2.2.1. Международный конфликт как процесс

Выделяя конфликт из процесса международных отношений, приходится совершать осознанные округления, из которых можно вычленить следующие их три вида:

- округление осуществляется в начале анализа. При этом все связи конфликта с системой международных отношений учитываются как связи объекта с внешней средой;
- округление связано с неполнотой и разной степенью достоверности любых знаний об объекте;

[45] См. Козер Л. А. Функции социального конфликта / Пер. с англ. О.Назаровой; Под общ. ред. Л.Г.Ионина. - М.: Дом интеллектуальной книги: Идея-пресс, 2000

[46] Бабинцев В.С. Методика слежения за развитием международных конфликтов и прогнозирование их развития // Моделирование процессов мирового развития и сотрудничества. - М.: 1991. С.72-74

- округление для построения формальной модели конфликта и его математической обработки.

Изучение конфликта как процесса позволяет проследить динамику его развития, которую условно можно разбить на фазы, каждая из которых представляет его состояние и имеет свое содержание и структуру, и может исследоваться как конфликтная ситуация.

Эскалационное развитие конфликта включает следующие фазы[47]:

1. Формирование у участников интересов и целей, столкновение которых приводит к возникновению противоречий между ними.
2. Поиск участниками путей достижения целей различными мирными методами и средствами (компромисс).
3. Формирование у прямых участников (или хотя бы у одного из них) путей и средств бескомпромиссного решения противоречий.
4. Вовлечение косвенных участников и формирование конфликтующих сторон.
5. Сознательное применение одной из сторон военной силы в демонстрационных целях или ограниченных масштабах в надежде принудить другую сторону к отказу от своих интересов и целей.
6. Кризис - вооруженное столкновение прямых участников с поддержкой косвенных участников (или разрыв отношений).

Деэскалационное развитие конфликта включает следующие фазы:

1. Отказ от ведения военных действий одной из сторон или обеими сторонами (капитуляция одного из участников, заявление одной или обеих сторон нести мирные переговоры или о временном прекращении огня).
2. Поиск конфликтующими сторонами компромисса. Частичное или полное достижение целей косвенных участников.
3. Поиск компромисса между прямыми участниками по поводу основного противоречия.
4. Достижение прямыми участниками компромисса.
5. Мирное разрешение противоречия - добровольный отказ одного или обоих участников от интересов и целей, составляющих противоречие.

Конфликт не обязательно должен включать все фазы эскалации и деэскалации, т.к. его развитие может протекать настолько сложно, что он может переходить от эскалационного к деэскалационному и обратно.

На практике даже острые противоречия не всегда выливаются в

[47] Здравомыслов А.Г. Социология конфликта. - М.: 1995. С. 53-55

вооруженную борьбу. При анализе кризиса необходимо учитывать и возможность полного разрыва отношений между его участниками, которые могут прибегать также к экономической блокаде, вводить эмбарго и иные дискриминационные меры.

Кроме того, конфликт, возникший по поводу одних противоречий, может потерять остроту, однако он способен продолжаться, но уже по поводу других. **В силу этого при анализе конфликта важно выявить доминирующие противоречия, а при исследовании конкретного конфликта нельзя не учитывать воздействия на ход его развития случайных факторов**.

2.2.2. Международный конфликт как ситуация. Основные компоненты конфликта

Международный конфликт характеризуется признаками, с помощью которых он может быть выделен из системы международных отношений. Анализ конфликта как набора следующих друг за другом фаз дает онтологическую, описательную картину со следующим порядком исследования: изучение и анализ зафиксированной конфликтной ситуации, позволяющие выявить ее структурные компоненты, а также закономерности и тенденции[48].

Первый структурный компонент - это **участники конфликта**. В качестве его участников могут выступать:

- государственные образования (государства, межгосударственные союзы, межправительственные организации);
- негосударственные образования (партии, общественные движения, этнические группы, неправительственные организации).

В зависимости от того, какую роль участник играет в конфликте и какова его степень вовлеченности в конфликт, участники подразделяются на:

- прямых участников;
- косвенных участников;
- посредников.

Следующей структурной компонентой являются **интересы участников**, например:

- экономические;
- политические;
- сырьевые;

[48] Сетов Р.А. К вопросу о понятии конфликта в теории международных отношений // Российская американистика в поисках новых подходов. Материалы научной конференции ассоциации изучения США. Исторический ф-т МГУ им.М.В.Ломоносова. - М.: 1998. С. 67

- территориальные;
- геостратегические;

Их можно классифицировать по степени важности:

- жизненно важные интересы;
- важные интересы;
- менее важные интересы;
- интересы.

Столкновение интересов прямых участников международных отношений или, другими словами, дефицит того, что представляет взаимный интерес, порождает конфликт.

Для прогнозирования необходимо знать и учитывать степень важности интереса, т.к. это поможет рассчитать вероятность и меру возможной уступки со стороны того или иного участника.

За третью структурную компоненту принимаются **ресурсы участников конфликта**:

- политические;
- экономические;
- валютно-финансовые;
- дипломатические;
- идеологические;
- военные;
- информационные.

Исходя из ресурсов, участник конфликта формирует свои цели, которые являются четвертым элементом международной конфликтной ситуации.

Сформулированные цели представляют собой тактику реализации стратегических интересов. По мере развития конфликта цели участников, как прямых, так и косвенных, могут меняться. Это связано с тем, что ресурсы, которыми располагают участники, и сама ситуация, диктующая возможность или невозможность применения тех или иных средств и достижения поставленных целей, могут меняться.

Определив цели участников, можно разделить остальных акторов на союзников и соперников. Эта категория также является подвижной.

Другой важной характеристикой конфликтной ситуации является **масштаб конфликта**, под которым подразумевается количество государств, на территорию которых распространяется конфликт:

- макроконфликт (глобальный или планетарный);
- гиперконфликт (континентальный или мировой);
- региональный конфликт;

- субрегиональный конфликт;
- миниконфликт.

Косвенные участники конфликта характеризуются степенью вовлеченности в конфликт. **Форма вовлеченности** в конфликт может быть:

- политическая;
- экономическая;
- полувоенная;
- непосредственное военное вмешательство.

Уровень участия:

- низкая степень вовлеченности.
- средняя степень вовлеченности;
- высокая степень вовлеченности.

Для описания конфликтной ситуации необходимо выявить основные **причины конфликта**[49], к которым относят:

- дефицит ресурсов;
- социальную напряженность;
- терроризм;
- нарушение прав человека;
- религиозные и этнические разногласия;
- чрезмерный уровень милитаризации;
- высокий уровень криминализации государства.

Важной характеристикой является **потенциал конфликта**. Под ним понимается уровень обострения противоречий, определяемый привлекаемыми средствами, ресурсами и возможностями их пополнения и выражающийся вероятностью перерастания конфликта в кризисную фазу.

Качественной характеристикой потенциала конфликта является **напряженность** отношений между его участниками. Например, напряженность между государствами в политической сфере оценивается по характеру дипломатических и межправительственных связей, по ясности и решительности высказываний и заявлений руководителей государств, по информационной активности. В экономической сфере напряженность определяется по характеру валютно-финансовых, торговых, научно-технических связей; в военной сфере - по уровню мобилизационной готовности государств, по нацеленности и уровню подготовки их экономики к ведению военных действий, по стремлению к демонстрации достижения целей военными методами и средствами.

[49] Woodcock A.A. Conglict Structure Code for Conflict Definition and Resolution // The Cornwalls Group II: Analysis for and of the Resolution of Conflict. The Lester B. Pearson Canadian Int. Peacekeeping Training Centre, 1998. P. 144-160

К количественным характеристикам относятся[50]:

- количество людей, участвующих в конфликте;
- основной тип оружия, использующийся в конфликте;
- финансовые средства, затрачиваемые участниками.

Потенциал конфликта определяется также **направленностью отношений** между его участниками, которая определяется степенью готовности того или иного участника усилить напряженность отношений.

Уровнем напряженности можно измерять величину потенциала конфликтной ситуации (с определением вероятности перехода конфликта в кризисную ситуацию, для чего могут быть применены как математические методы, так и экспертные оценки). На рост напряженности конфликта влияет степень консолидации сил прямых и косвенных участников, составляющих два противоборствующих лагеря. Чем выше степень их консолидации, тем выше уровень напряженности конфликта.

Для получения перечисленных сведений необходим **информационный мониторинг** за развитием конфликта. При этом конфликтолог сталкивается с трудностями, связанными с большим объемом информации, с ее субъективным, нередко противоречивым характером, с информационным дефицитом, связанным не только с недостатком сведений, но и их низкой достоверностью.

Сегодня сбор и обработку информации, т.е. контент- и ивент-анализ осуществляют информационно-аналитические системы (ИАС, подробнее - в гл.4). Информация характеризуется двумя основными факторами - это степень ее достоверности и сведений о содержании и значении признаков и показателей собранной информации.

Матрица размещения компонентов конфликта, предложенная И.С.Бабинцевым[51], иллюстрирует степень изменчивости показателей и признаков структурных компонентов.

Трудностью в моделировании конфликта является представление суждений в виде числовых значений. **При попарных сравнениях двух сложных объектов непросто передать в виде точных цифр чувства и опыт по поводу того, на сколько влияние од-**

[50] Kilgour D., Hipel K., Fang L., Peng X. Applying the Decision Support System GMCR II to Peace Operation // The Cornwalls Group II: Analysis for and of the Resolution of Conflict. The Lester B. Pearson Canadian Int. Peacekeeping Training Centre, 1998. P. 29-47

[51] Бабинцев В.С. Методика слежения за развитием международных конфликтов и прогнозирование их развития. // Моделирование процессов мирового развития и сотрудничества. - М.: 1991. С. 76, 87

ного из объектов на достижение некоторой цели больше, чем второго.

Для распределения объектов по рангированию важности используется метод с определением числового значения. По мере накопления информации первоначальная шкала, выбранная для попарных сравнений, может быть модифицирована. Для того, чтобы представить результат сравнения двух объектов в виде цифр, требуется их глубокое осмысление и, особенно, в какой степени их свойства влияют на достижение рассматриваемой цели. Источником суждений является опрос экспертов по сравниваемым объектам, с целями и с их взаимосвязью. Построение шкалы важности объектов начинается с выделения рангов важности.

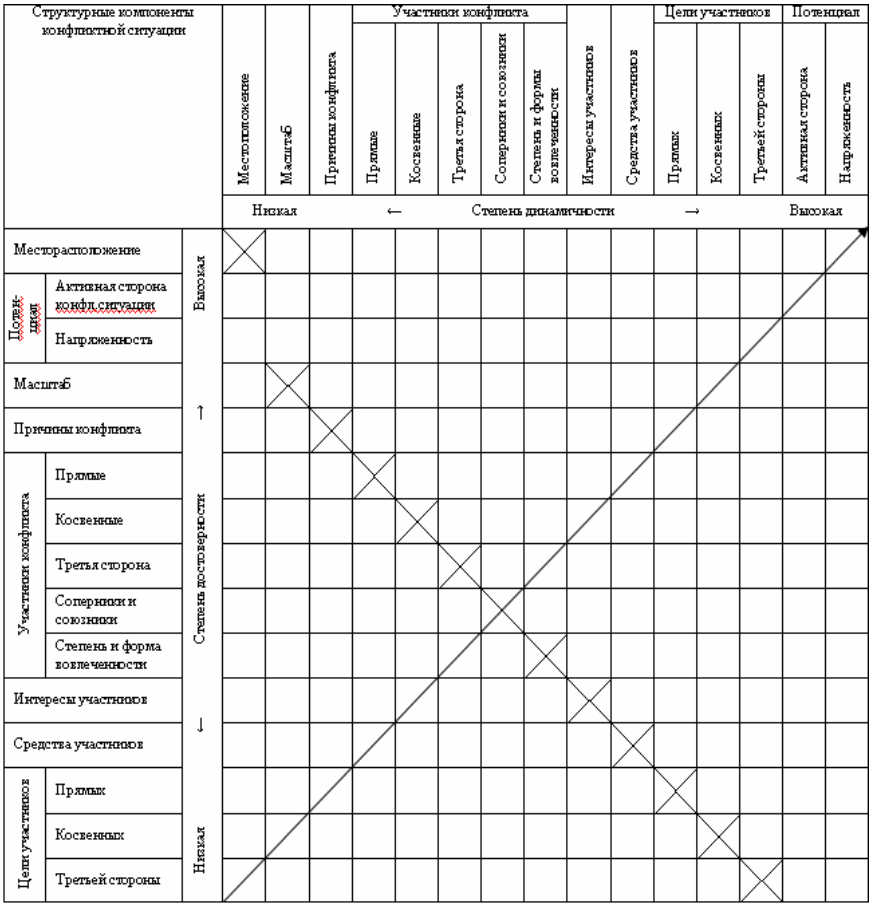
Таблица рангов важности

Степень важности	**Определение**	**Пояснения**
0	Объекты несравнимы	Сравнение двух объектов бессмысленно
1	Объекты одинаково важны	Оба объекта вносят одинаковый вклад в достижение поставленной цели
3	Один немного важнее другого	Есть некоторые основания предпочесть один объект другому, но их нельзя считать неопровержимыми
5	Один существенно важнее другого	Существуют веские свидетельства того, что один из объектов более важен
7	Один явно важнее другого	Имеются неопровержимые основания, чтобы предпочесть один другому
9	Один абсолютно важнее другого	Превосходство одного из объектов столь очевидно, что не может не вызвать ни малейшего сомнения
2, 4, 6, 8	Значения, предписываемые промежуточным суждениям	Используются, когда выбор между двумя соседними нечетными числами вызывают затруднение
Числа, обратные к вышеперечисленным	Если при сравнении с объектом **j** объект **i** получил один из вышеуказанных рангов важности, то **j** при сравнении с **i** получает обратное значение	
Рациональные значения	Получаются при арифметических операциях с числами данной шкалы	

Далее по таблице составляется матрица сравнений[52], которая необходима для создания формальной модели.

Выводы можно получить, если построить матрицу размещения компонентов конфликта, в которой по столбцам по нарастающей степени изменчивости показателей расположить структурные компоненты конфликта, а по строкам их же по нарастающей степени достоверности сведений и сообщений о показателях и признаках.

Матрица размещения компонентов конфликтной ситуации



[52] Саати Томас Л. Математические модели конфликтных ситуаций. - М.: 1977. С. 34-37

Стрелка по диагонали матрицы указывает на нарастание полезности информации для анализа и прогнозирования конфликта.

В матрице выделяют две зоны наблюдения: основную и дополнительную. В основной зоне располагается структурный компонент «потенциал конфликтной ситуации», в дополнительной - «участники конфликта», «средства участников», «цели участников», «интересы участников», «масштаб конфликта», «причины конфликта».

Таким образом, **из всех компонентов конфликта наиболее динамичные признаки и показатели имеет его потенциал**.

Выбор напряженности потенциала конфликта в качестве показателя слежения за состоянием конфликта определяется следующими факторами:

- реагированием на любые действия конфликтующих сторон;
- широким спектром информационных потоков;
- возможностью непосредственного измерения;
- высокой достоверностью.

2.3. Типология конфликтов

Как уже отмечалось, коренное изменение в исследованиях мира и конфликтов на Западе произошло в 1960 г., когда норвежец И.Галтунг вместо фокусирования на исследованиях причин конфликтов обратил внимание на изучение условий для создания мира. **Считается, что именно с этого момента теория конфликта и теории мира были слиты воедино**. И.Галтунг сравнивает исследования и практику по урегулированию конфликтов с медициной, где выделяются три основных задачи:

- диагностика;
- составление прогноза;
- терапия.

В многообразии конфликтов исследования стали выявлять не уникальные особенности конкретной ситуации, а, напротив, принципиально новые моменты, позволяющие разрешать их мирными средствами.

2.3.1. Конфликты согласно классификации ООН

Принцип мирного разрешения международных споров сформировался еще до второй мировой войны[53]. В дальнейшем он был конкретизирован и развит в Уставе ООН (п. 2 ст. 2, ст. 33-38 Устава ООН). Единственно правомерным способом решения споров и разногласий между государствами объявляются мирные средства, перечень которых дан в Уставе ООН. Международные споры разрешаются на основе суверенного равенства государств и при соблюдении принципа свободного выбора средств в соответствии с Уставом ООН и принципами справедливости и международного права. При этом применение какой-либо процедуры урегулирования спора или согласие на такую процедуру, согласованную между государствами в отношении споров, в которых они являются сторонами, не должно рассматриваться как несовместимое с принципом суверенного равенства государств.

Устав ООН классифицирует споры на следующие две категории:

а) особо опасные, продолжение которых может угрожать поддержанию международного мира и безопасности (ст. 34);

б) любые другие споры (п. 1 ст. 33,. п. 1 ст. 35, п. 1. ст. 36).

Наряду с термином «споры» в Уставе ООН имеется понятие «ситуация» (ст. 34, п. 1 ст. 33). Ситуация также «может привести к международным трениям» или вызвать «спор». Устав ООН не содержит критериев разделения споров и ситуаций на вышеуказанные две категории, относя решение этого вопроса к компетенции Совета Безопасности. Ст. 34 Устава ООН гласит: «Совет Безопасности уполномочивается расследовать любой спор или любую ситуацию, которая может привести к международным трениям или вызвать спор, для определения того, не может ли продолжение этого спора или ситуации угрожать поддержанию международного мира и безопасности».

Таким образом, деление международных конфликтов на «споры» и «ситуации» является условным и относительным.

Ситуация - более широкое понятие, чем спор. Устав ООН, а также другие международные договоры не содержат четкого разграничения между политическими и юридическими спорами. Согласно п. 3 ст. 36 Устава ООН споры юридического характера должны, как правило, передаваться сторонами в Международный

[53] Хохлышева О.О. Мир данности и иллюзии миротворчества. Нижний Новгород. 1996. С.49

Суд. Статут Суда содержит перечень правовых споров, по которым юрисдикция Суда является обязательной.

Перечень мирных средств, предусмотренных в Уставе ООН, не является исчерпывающим, а некоторые из них являются декларативно-рекомендательными. **В этой связи СССР, в своем Меморандуме о повышении роли международного права, представленном на 44-й сессии ГА ООН 29 сентября 1989 г., предложил выработать и принять универсальный международно-правовой акт, который стал бы действенным инструментом по укреплению международного правопорядка**.

2.3.2. Два основных вида вооруженных конфликтов

В международном праве различают два основных вида вооруженных конфликтов: **международный вооруженный конфликт и вооруженный конфликт немеждународного характера**. Особую категорию составляют интернационализированные внутригосударственные конфликты.

Международный конфликт рассматривается в качестве особого политико-правового отношения двух или нескольких сторон - народов, государств или групп государств, имеющих косвенные или непосредственные столкновения интересов, целей, объективные и субъективные экономические, социально-классовые, политические, идеологические, территориальные, национальные (племенные), религиозные или иные по своей природе и характеру противоречия и отношения.

При этом принцип неприменения силы означает, что с начала войны и до урегулирования конфликта стороны, с точки зрения международного права, находятся в неравном положении. **Действия стороны, применившей силу, рассматриваются как агрессия, а действия защищающейся стороны - как самооборона. Основным критерием оценки действий государства в качестве акта агрессии является применение силы первым.** Агрессия оправдывает ответное применение силы со стороны жертвы агрессии, которая, согласно ст. 51 Устава ООН, обладает неотъемлемым правом на индивидуальную или коллективную самооборону.

Межгосударственный конфликт по своей сути несовместим с международным правом, которое запрещает государствам использовать силу в отношениях друг с другом (пункт 4 статьи 2 Устава ООН гласит, что все члены ООН воздерживаются в их международных отношениях от угрозы силой или ее применения как против

территориальной неприкосновенности или политической независимости любого государства, так и каким-то другим образом, несовместимым с целями ООН).

Вооруженный конфликт немеждународного характера, в соответствии с п. I ст. 1 Дополнительного протокола II к Женевским конвенциям 1949 г., - это вооруженный конфликт, происходящий на территории какой-либо из Высоких Договаривающихся Сторон между ее вооруженными силами или другими организованными вооруженными группами, которые, находясь под ответственным командованием, осуществляют такой контроль над частью ее территории, который позволяет им осуществлять непрерывные и согласованные военные действия и применять Протокол II.

Интернационализированный внутренний вооруженный конфликт - политико-правовое явление системы международных отношений новейшего времени. При этом можно выделить следующие его причины:

1. Возросшая взаимозависимость государств.
2. Идеологические расхождения между государствами.
3. Существование военно-политических блоков и группировок государств, заинтересованных в стабилизации положения дел внутри своего блока и стремящихся к дестабилизации политических режимов в других образованиях[54].

2.3.3. Структура и новый характер конфликтов

Структура межгосударственного конфликта определяется тремя основными элементами: конфликтная ситуация и конфликтное поведение, взаимодействующие через среду, а также сама среда.

Наличие сторон является необходимым, но не определяющим условием конфликта, так как нужны еще три его элемента: столкновение интересов, конфликт позиций и конфликтное поведение сторон. Столкновение интересов и конфликт позиций рассматриваются в рамках конфликтной ситуации.

По мнению М.Болдуина, **конфликтная ситуация - это любая ситуация, при которой стороны (независимо от состава) осознают, что обладают несовместимыми целями**[55].

[54] Егоров С.А. Вооруженные конфликты и международное право. М.: 1999. С. 49

[55] Современные буржуазные теории международных отношений. М.: Издательство «Наука», 1976. С. 382

Характер сталкивающихся интересов сторон определяет и характер потенциального конфликта. Основные категории интересов:

- индивидуальные интересы отдельных государств (идеологические, классовые, религиозные и иные, объединяющие противостоящие блоки);
- групповые интересы;
- коллективные (общие) интересы государств как участников международной системы.

Потенциальной возможностью столкновения обладают первая и вторая категории интересов. Третья категория, предопределяя ту или иную степень интеграции сторон, ослабляет интенсивность существующих противоречий.

Если противоречия между сторонами опосредует столкновение индивидуальных и групповых интересов, то это худший вариант[56]. В теории это получило название игры с нулевой суммой, при которой приобретение одного участника равно потере другого, а когда они вместе, то их сумма равна нулю.

Столкновение национальных интересов может быть даже в условиях военно-политического единства государств. Например, противоречия между странами-участницами НАТО Грецией и Турцией.

Различия можно выразить в общем виде через системы ценностей. **Конфликт ценностей возникает при наличии принципиальной разницы в системах ценностей, что ведет к открытой несовместимости целей, интересов.** Единой ценностью обладают статус, роль на международной арене, ресурсы, которые, как правило, и являются предметом конфликта.

Разграничение интересов на существенные и специальные подразделяется Уставом ООН на «политические» и «правовые» споры.

Исследуемый конфликт можно представить следующим образом:

- определение цели;
- способ ее достижения;
- определение причин, вызвавших негативное явление;
- способы его преодоления.

Первый идентификатор определяет тип целей конфликта:

- позитивные:
- негативные.

Этим типам соответствуют различные психологические модели конфликта (сближение, избегание).

[56] Закажурников С.Ю. Методика анализа межгосударственного конфликта. С. 25, 28, 36

Английский конфликтолог Дж.Френкель считает, что первый уровень, на котором возникает проблема разрешения конфликта, состоит в определении интересов и целей. Далее он выделяет **три вида целей: победа, власть, мир**[57].

- цель либо никогда не будет достигнута, либо должна привести к уничтожению соперника. Это говорит о том, что **победа базируется на интересах, приводящих к игре с нулевой суммой, в которой задачи сторон направлены на уничтожение, подчинение или изоляцию противника.**

- в отличие от победы, **обеспечение власти оставляет структуру, хотя и призвано создать позицию для возможного в будущем изменения этой структуры в пользу преобладающей в конфликте стороны.** Такую цель можно назвать преобладанием, подчеркивая то, что в случае столкновения индивидуальных существенных интересов, эти столкновения, в итоге, могут быть разрешены соглашением сторон, но за счет уступки одной в пользу другой.

- **целью может быть мир, когда стороны подтверждают незыблемость системы без ущерба для позиций каждой из них.**

Источники несовместимых целей:

- недостаток материальных ценностей;

- проблемы статусного характера.

Важное место в конфликте занимают установки, которые включают в себя эмоции, склонности к пассивному, активному или агрессивному образу действий. Они определяются характером взаимоотношений сторон конфликта: является ли он дружественным или враждебным, носит ровный или напряженный характер.

Вторым важным элементом структуры является конфликтное поведение.

Конфликтное поведение - действия одной из сторон, выходящие за рамки нормативного межгосударственного общения.

По определению Рапопорта, в «борьбе», «игре», «дебатах» конфликты типа «борьба» решаются силой, «игра» оканчивается в пользу одной из сторон, «дебаты» завершаются на основе консенсуса[58].

Направленность конфликтного поведения:

- соперничество (направленность на достижение целей, находящихся вне сторон);

---

[57] Современные буржуазные теории международных отношений. М.: Издательство «Наука», 1976. С. 382

[58] Скакунов Э.И. Международно-правовые гарантии безопасности государств. М.: Издательство «Наука», 1983. С. 85

- конфликт (направленность друг на друга);
- направленность поведения на цели оппонента.

Целесообразность открытой конфронтации для одной из сторон определяется формулой:

$$\mathbf{PV - RC > 0}$$

где:

V – ценность цели, достигаемой путем нападения;

P – вероятность достижения цели путем нападения;

C – возможные потери в ходе нападения;

R – вероятность того, что потери будут иметь место.

Для противоположной стороны существует четыре пути удержать своего оппонента от нападения: путем снижения **V** и **P,** увеличения **C** и **R**.

Снижение привлекательности цели заключается в том, что даже в случае удачи полученная выгода не будет стоить затрат.

Снижение **P**, по существу, означает меры другой стороны по пропаганде ее оборонительных возможностей.

Увеличение **C** состоит в убеждении в серьезности потерь, которые может понести агрессивная сторона.

Потенциальной жертве агрессии, для увеличения **R** необходимо убедить противника в решимости осуществить ответные действия.

Типы поведения:

- непосредственное поведение выражается в стремлении очевидного навязывания условий противоположной стороне;
- угроза ухудшить положение стороны своими действиями;
- сковывающее поведение;
- действия, направленные на удержание конфликта на существующем уровне эскалации.

Последним элементом структуры конфликта является среда конфликта - набор факторов протекания межгосударственного конфликта.

Взаимовлияние структур конфликта обеспечивается тем, что при анализе каждого последующего элемента учитываются результаты анализа предыдущих. Структура конфликта исследуется как показатель связей в системе элементов, которую можно классифицировать следующим образом:

1) выявление связи между двумя элементами системы;
2) связи одного элемента с набором различных элементов;
3) связи одного элемента с множеством элементов;
4) связи одного или нескольких групп элементов.

Необходимо заметить, что на практике решение этих задач вызывает значительные трудности, т.к. в новой структуре конфликта

порой невозможно точно определить элементы: конфликтную ситуацию, конфликтное поведение и стороны в конфликте.

При проявлениях в зоне конфликта терроризма, особенно международного, все труднее поддаются количественному анализу его участники и стороны. С учетом роста террористического потенциала в мире, в т.ч. кибертерроризма, традиционные методы анализа конфликта эффективны лишь в комбинации с инновационными методами.

В вооруженных силах ведущих государств широким потоком внедряются новые технологии ведения боевых действий. Планируются и отрабатываются модели войн XXI века. Армии крупнейших государств модернизируются, исходя из установки на решительную победу в будущих войнах. Переход к несиловой цивилизации, о котором говорилось в канун XX века, отодвигается на неопределенное время.

2.3.4. Наследие Клаузевица и современные войны

Война, как ее видел Клаузевиц, велась профессиональными армиями или армиями на основе призыва во имя государства. **Новые войны, как правило, направлены на дезинтеграцию и эрозию госструктур**, в них:

1. Нет изначальной идеи «государства».
2. «Возвращение» к «трайбализму», «примитивизму», «вековой этнической вражде».
3. Возрождение догосударственных структур.

Новые войны[59]**:**

1. «Более продолжительны и масштабны, рост соотношения жертв по категории «гражданские-военные».
2. Нет явного «победителя» и «побежденного».
3. Децентрализованные и разрозненные «боевые действия».
4. Цель: дестабилизация и перемещение гражданских групп по сравнению с уничтожением целей противника.
5. Задача: сеять рознь, разрушать мораль, моральные устои, разрушать социально значимые священные устои, подрывать верховенство права, уничтожать надежду.
6. Средства: зверства, приковывающие к себе внимание, голод, осада.
7. Цели: больницы, школы, рынки и т.д.

[59] Информационные войны рассматриваются в § 5.4.

Новая группа действующих лиц:

1. Племена, кланы, семьи и группы.
2. Организованные криминальные элементы.
3. Полувоенные формирования.

Возникновение класса боевиков, которые:

1. Молоды и не имеют опыта.
2. Не имеют иллюзий и не заинтересованы в мире.
3. Не имеют надежд: нет перспектив.
4. Имеют признание среди «обиженной» властями части населения, инспирируемое чувство товарищества.

«Де-эволюция» военного дела:

1. Негражданские «гражданские» войны.
2. Асимметричные противники.
3. Урбанизированная война: много некомбатантов.
4. Дилемма: национальное против человеческого интереса
5. Современные технологии в военной сфере соседствует с ближним боем.
6. Утрата «рациональности» конфликта.
7. Приверженность принципу верховенства права делает солдат беззащитными.

Генезис конфликта 21 века:

1. Острова богатства в море сохраняющейся бедности.
2. Нетрадиционные империи.
3. Борьба за гегемонию ресурсов.
4. Возвращение к догосударственным структурам.
5. Стирание различия между военными операциями и обеспечением правопорядка.
6. Появление класса «боевиков».
7. Непредсказуемое сочетание антропогенных, природогенных и социогенных катаклизмов и коллизий.

Источники будущих конфликтов

1. Конфликты будут порождаться разрушением и эрозией госструктур.
2. Рост деспотизма и коррупции.
3. Фрагментация контроля за насилием.

Причины новых войн:

Роль политики идентификации

1. Политика идентификации - средство мобилизации широкого диапазона интересов.
2. Политика идентификации, т.е. принадлежности к определенной этнической группе (в форме культуры, языка или верования).

3. Право по рождению, а не по выбору, как в случае с религией, идеологией и т.п.

4. Исключительность, например, право на территорию, в т.ч. с фальсификацией исторических фактов.

5. Имманентно содержит элементы исключительности и сепаратизма.

Глава 3
ИННОВАЦИОННЫЕ МЕТОДЫ АНАЛИЗА ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ

Невозможно решить проблему,
находясь на том же уровне сознания,
на котором мы ее создали.

А.ЭЙНШТЕЙН

3.1. Метод ситуационного анализа (опыт академика Е.М.Примакова)

Метод, объектом исследования которого является международный конфликт, разработан коллективом авторов во главе с академиком Е.М.Примаковым еще в 1970-е гг. и был удостоен Государственной премии СССР.[60]

Ситуационный анализ (СА) позволяет организовывать и направлять процесс сбора, оценки и обработки информации для генерации оценок как аналитического, так и прогнозного характера.

СА проводится в три этапа с участием 10 - 15 экспертов.

На первом этапе назначается эксперт-руководитель СА и создается группа экспертов (до шести чел.). Эта сценарно-редакционная группа уточняет формулировку темы (задания), разрабатывает и представляет на утверждение установочную записку и сценарий, анкеты для формализованного опроса экспертов, а также подбирает экспертов для второго этапа СА. Сценарий представляет собой дробление исследуемой проблемы на ряд подпроблем, которые, в свою очередь, разбиваются на еще более мелкие подпроблемы и так далее. Каждая подпроблема любого уровня при разбиении должна члениться на непересекающееся множество подпроблем следующего уровня.

В целом сценарий схематично представляет собой дерево с одним корнем (нулевой уровень). В идеальном случае (если в ходе экспертизы не появится необходимости переструктурирования проблемы) сценарий одновременно становится итоговым документом.

---

[60] См. Ю.В.Сидельников.
http://www.maib.ru/prognostication/methodsandmodels/methodsandmodels_15.html

Проблемы самого нижнего уровня формулируются как вопросы к экспертам.

Совокупность вопросов, зафиксированная и утвержденная редакционной группой, представляется как анкета на втором этапе СА. Второй этап начинается с информации руководителя-эксперта. Он напоминает основные правила проводимой экспертизы:

- экспертиза неофициальна, поэтому каждый эксперт высказывает не точку зрения своей организации, а исключительно свое личное мнение;

- экспертиза анонимна в том смысле, что в итоговом документе высказанные точки зрения не соотносятся с конкретными фамилиями;

- экспертиза конфиденциальна, поэтому содержание выступлений и сам факт проведения СА не подлежат разглашению ни устно, ни в открытой печати, а конспектирование в ходе коллективной экспертизы и вынос анкет формализованного опроса не разрешаются.

Затем эксперты поочередно выступают с десятиминутным «домашним заданием». Их выступления основываются на заранее разосланных им материалах (включая анкету). Эксперты озвучивают возникшие у них вопросы и обсуждают полученные ответы. Цель второго этапа - получение большого объема экспертных оценок индивидуального и коллективного характера.

На третьем, заключительном этапе СА редакционно-сценарная группа, включающая по желанию руководителя и экспертов из основной группы, готовит заключительный аналитический документ. Руководитель СА утверждает его окончательную редакцию.

В 2006 г. издательство МГИМО(У) выпустило работу Е.М.Примакова «Методика и результаты ситуационных анализов мастер-класс по программе Мировая политика»[61]. Данная работа стала результатом проведения мастер-класса Е.М.Примаковым для студентов магистратуры по международным отношениям МГИМО (У) (программа «Мировая политика») в 2003-2006 гг. В ней впервые представлено описание методики ситуационного анализа, приводятся примеры сценариев, а также результаты проведенных ситуационных анализов по проблемам ядерной программы Северной Кореи и ситуации в Ираке. Это позволяет использовать данную методику не только для изучения конкретных проблем Северной Кореи и Ирака, но и в качестве конкретного пособия для формирования

[61] Примаков Е.М Методика и результаты ситуационных анализов. Мастер-класс по программе «Мировая политика». М.: Изд-во МГИМО (У). 2006

практических и аналитических навыков при проведении ситуационных анализов, в т.ч. с использованием современных информационно-коммуникационных технологий.

3.1.1. Система ситуационных центров МГИМО(У)

МГИМО(У) располагает тремя ситуационными центрами (СЦ): политологическим, экономическим и энергетическим[62]. С учетом исследуемой проблематики рассмотрим лишь вариант использования СЦ для моделирования.

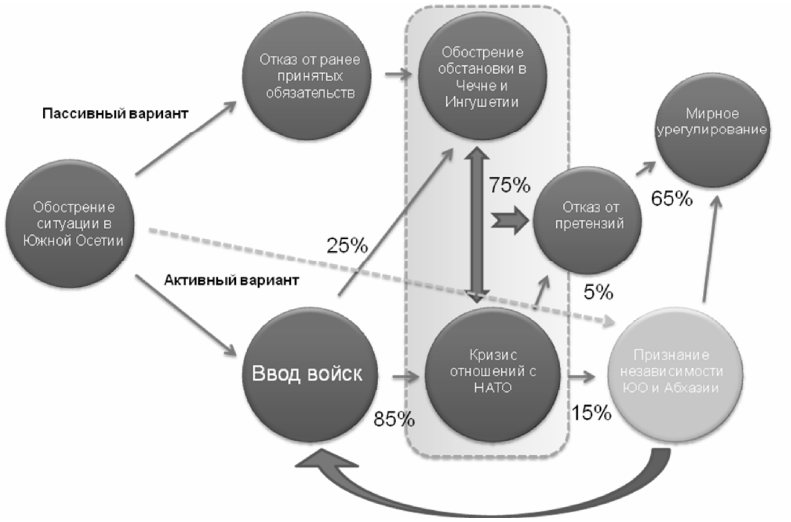
- В моделировании могут принять участие по 13 чел. в каждом СЦ.
- Все участники подключены к Интернету, к базам знаний, а также имеют аналитические инструменты и электронные справочники.
- Моделирование может проводиться в реальном времени.
- По разработанной экспертной модели моделирование может проводиться многократно без привлечения автора ситуации.
- Каждый узел ситуации имеет информпакет, имитирующий сообщения СМИ, аналитические записки, доклады и т.д.
- Система видеоконференцсвязи (ВКС) позволяет привлекать к моделированию внешних специалистов.
- Беспроводная ЛВС позволяет привлекать к моделированию до 25 наблюдателей в каждом СЦ.
- Из любого СЦ возможно наблюдение за моделированием в другом СЦ.
- Система визуализации позволяет выводить информацию с рабочих мест, с видеокамеры, а также с подсистемы ВКС.
- Система протоколирования сессий моделирования ведет его полную запись для последующего анализа и оценивания.

Кроме офисных пакетов в АРМ СЦ имеется:

- Настольная персональная версия ГИС ArcInfo.
- Клиент системы «Семантический архив».
- Клиент системы геополитического анализа.
- Система «Медиалогия».
- Электронные библиотеки.

[62] http://www.mgimo.ru/files/31114/SC_concept.doc

3.1.2. Пример ситуационного моделирования агрессии Грузии (2008 г.)



3.2. Ситуационно-кризисный центр как инструментарий конфликтолога

В условиях роста конфликтного потенциала в мире резко возросла роль ситуационно-кризисных центров (СКЦ), оснащенных новейшими информационными и управленческими технологиями. Суть использования СКЦ заключается в возможности вести проблемный мониторинг, находить оптимальные варианты кризисного реагирования, а также моделировать и прогнозировать кризисы.

Согласно Стратегии национальной безопасности Российской Федерации до 2020 года (п.107), информационно-аналитическая поддержка управленческой деятельности должна осуществляться с использованием системы распределенных СКЦ, работающих по единому регламенту взаимодействия.

Понятие СКЦ связано с поддержкой принятия решений в кризисных ситуациях и/или обсуждения и решения многоаспектных политических, экономических и иных проблем. Часто в смысл СКЦ вкладывается сам процесс мониторинга развития различных ситуаций.

В зависимости от предметной области название «ситуационно-кризисного центра или комнаты» (situation room) может трансформироваться в «центр командования и управления» (command and control center), «кризисный центр» (crisis center), «чрезвычайный центр» (emergency center), «зал совещаний» (corporate boardroom, conference room). При этом под центром понимается не только специально оборудованное помещение, но и соответствующие информационные, телекоммуникационные, программные и методические средства, обеспечивающие процесс доставки и агрегирования информации, а также процесс ее интеллектуального обсуждения участниками анализа с целью выработки соответствующего решения.

Таким образом, **ситуационно-кризисный центр является производным информационной и управленческой революций**.

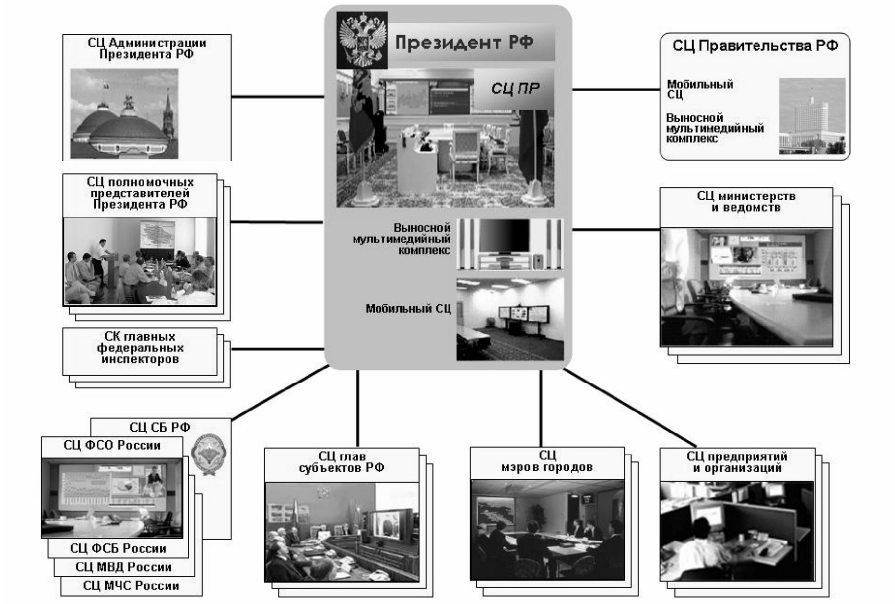
На сегодняшний день СКЦ существуют не только в госструктурах, но и в транснациональных корпорациях, крупных коммерческих организациях, где есть необходимость оперативного принятия управленческих решений на базе многоаспектной информации. В частности, ситцентры поддержки принятия решений оборудованы в компаниях PriceWaterHouse Coopers, Boeing, Aérospatiale, Nokia, Eastman Chemicals, Computer Science Corporation, Grenridge Insurance (Norway), во многих нефтяных корпорациях.

3.2.1. Система ситуационных центров органов государственной власти России

В настоящее время в России функционирует следующая система[63] взаимодействующих ситуационных центров органов госвласти, включающая в себя три уровня:

[63] Ильин Н.И. Развитие систем специального информационного обеспечения государственного управления / Ильин Н.И., Демидов Н.Н., Попович П.Н. -М.: Федеральная служба охраны Российской Федерации, 2009. - С.207.

Система ситуационных центров органов государственной власти Российской Федерации



Высший уровень - это ситуационный центр Президента России, который, наряду с аналогичными комплексами президента США и правительства Германии, является одним из наиболее технически совершенных в мире. Работают ситуационные центры Администрации Президента и Правительства России. На втором уровне находятся ситуационные центры полномочных представителей Президента России в федеральных округах, руководителей министерств (Национальный центр управлениях в кризисных ситуациях МЧС России), агентств (Росатом) и служб. На третьем уровне - ситуационные центры глав субъектов Российской Федерации и муниципальных образований[64].

Важнейшими факторами, обеспечивающими активное внедрение СКЦ в практическую деятельность органов госуправления, являются:

- необходимость совершенствования управленческих процедур путем включения в них экспертов не только на этапе принятия, но и при выработке решения;

[64] См. Ильин Н.И. Современные тенденции развития информационных систем органов государственной власти // Ситуационные центры 2009. Перспективные информационно-аналитические материалы научно-практической конференции РАГС. 14-15 апреля 2009 г.; Под общ.ред. А.Н.Данчула. - М.: РАГС, 2010. С.23.

- возможность оптимизации принимаемых решений путем их экспертной оценки и моделирования ситуации в реальном масштабе времени;

- возможность повышения качества предварительного анализа информации и вырабатываемых решений путем использования ИКТ, обеспечивающих интеграцию результатов аналитической обработки с полиэкранной формой визуализации информации;

- необходимость обеспечения лиц, вырабатывающих и принимающих решения, достоверной и полной информацией, представляемой в оперативном режиме;

- возможность оперативного доступа первого лица в сжатые сроки ко всей информации, относящейся к проблеме, требующей решения.

С учетом особенности и проблем функционирования СКЦ ОГВ наиболее перспективными являются следующие направления их развития:

- совершенствование и равномерность развития программно-технических компонентов, создание единой структуры и технологии информационного обеспечения выносных мультимедийных комплексов, обеспечение оперативной и актуализированной информацией выносных мультимедийных комплексов руководителей верхнего звена;

- использование режима видеоконференции, внедрение современных интегрированных систем управления презентациями, полиэкранные формы представления информации;

- обеспечение информационной интеграции, как по вертикали управления, так и по горизонтали, создание единой технологии информобмена между объектами управления, организация и наполнение интегрированной мультимедийной базы данных;

- разработка типового состава ИАС и баз данных общего назначения, что обеспечит информационное взаимодействие между объектами управления;

- оснащение СКЦ справочной и нормативно-правовой системой, ГИС, мониторинговыми системами производственных, экономических, социальных, инвестиционных и финансовых ситуаций.

Однако в настоящее время в России существует ряд проблем в создании СКЦ, в т.ч. и на государственном уровне. Для развития системы распределенных СКЦ в среднесрочной перспективе потребуется преодолеть технологическое отставание в важнейших областях информатизации, телекоммуникаций и связи, определяющих состояние национальной безопасности, разработать и внедрить технологии информационной безопасности в системах государствен-

ного и военного управления, системах управления экологически опасными производствами и критически важными объектами, а также обеспечить условия для гармонизации национальной информационной инфраструктуры с глобальными информационными сетями и системами.

С технологической точки зрения СКЦ любой организации являются составными частями его информационно-телекоммуникационной системы (ИТКС) и мало чем отличаются от СКЦ государственных структур. При этом используются самые современные ИКТ (Интернет/Интранет порталы, аналитические программы и базы данных, мультимедийные, в т.ч., источники видеоинформации, геоинформационные системы, видеоконференцсвязь, «умные» средства отображения и т.п.).

Существует ряд признаков «ситуационности» проблемы, указывающих на целесообразность их решения с помощью информационно-аналитических технологий, поддерживаемых СКЦ:

- концептуальность описания проблемы;
- неформализуемость, неопределенность;
- взаимовлияние множества факторов;
- большие объемы неявной информации;
- хаотичность изменения ситуации.

Среди основных целей создания ситуационно-кризисных центров выделяют следующие:

- интеграция информресурсов ИТКС предприятия, включая мультимедийные источники, для обеспечения информационной поддержки деятельности руководства Предприятия;
- наглядное и рациональное представление многоаспектной информации, в т.ч. в режиме он-лайн с лент мировых агентств, финансовых структур и т.п. с использованием современных средств отображения;
- организация и обеспечение технологической поддержки проведения совещаний, коллегий и т.п. с использованием современных методик коллективной работы, включая методы «мозгового штурма» и т.п., протоколирование проводимых мероприятий;
- обеспечение возможности удаленного подключения и эффективной работы распределенных групп экспертов;
- обеспечение возможности эффективного и оперативного управления руководителем предприятия своими подразделениями, в т. ч., удаленными, путем личного визуального контакта;
- обеспечение непосредственного доступа руководства и специалистов предприятия к достоверной информации из различных

источников с выдачей ее на один экран (реализация принципа «единого окна»), улучшение представления отчетной информации;

- повышение оперативности и качества управленческих решений на основе использования аналитических и прогнозных средств;

- совершенствование взаимодействия с ситуационными центрами и аналитическими структурами других предприятий и ведомств.

В настоящее время существуют два подхода построения СКЦ: локальный и распределенный.

Перспективным является построение распределенного СКЦ По сути, это - совокупность связанных между собой ситцентров, ориентированных на реализацию концепции управлениями знаниями. При этом физически (как объект) может существовать один центр, но технологически и информационно имеется возможность организации работы виртуальных групп экспертов (участников ситанализа).

Кроме того, оснащение и методическое обеспечение работы центра должно позволять не только реализовывать просмотр презентаций и заслушивание соответствующих докладов, но и проводить и в динамике обращаться к необходимым информационным источникам, анализировать альтернативные версии решений и т.п.

3.2.2. Основные модули СКЦ

СКЦ, как правило, включает в себя следующие модули**:**

- Комплекс технологических средств (КТС).
- Информационно-аналитические средства (ИАС) и интерфейсы.
- Организационно-административная компонента.

КТС должен обеспечивать возможность приема (получения) и выдачи (отображения) разнородной информации, поступающей как из внутренних источников, так из внешних.

ИАС обеспечивает интегрированную обработку поступающей информации, представление ее в форме, готовой для обсуждения и анализа. Интерфейсы должны обеспечивать связь с корпоративными и иными базами данных, а также семантическое единство представляемой информации.

Организационно-административная компонента обеспечивает управление КТС и ИАС, а также предоставляет информационную и аналитическую поддержку в режиме реального времени в процессе обсуждения и принятия решений.

Возрастание конфликтного потенциала в мире и рост информационных потоков во многом заставили переоценить как саму концепцию СКЦ, так и способы ее реализации. **В частности, используемые методы накопления информации, ее агрегирования и мониторинга не смогли обеспечить своевременного информирования руководства ряда стран о надвигающейся террористической угрозе.**

В прежнюю концепцию СКЦ была заложена технология **data management (управления данными) или information management (управления информацией)**. По сути, деятельность СКЦ сводилась к отображению информации для ее обсуждения по заранее спрогнозированному сценарию.

Технологии knowledge management (управление знаниями) позволяют перейти к реальной генерации в СКЦ управленческих решений. В основу этой технологии положена возможность накопления знаний о решениях в подобных ситуациях, накопление знаний и сведений о людях (организациях), способных стать экспертами в той или иной области.

Активно развивается направление видеоконференций, использование которых позволяет расширить состав привлекаемых к обсуждению экспертов (многие из них не приглашались по причинам объективного ограничения состава участников).

При этом развивается направление оказания внешних (по отношению к владельцу СКЦ) услуг (outsourcing) сторонними организациями как в части привлечения их экспертов к анализу проблемы (ситуации), так и в части использования их вычислительных мощностей для накопления и мониторинга соответствующей информации. Перспективным видится использование «облачных» технологий.

СКЦ выступает в качестве инструмента, позволяющего лицу, принимающему решение (ЛПР) оперативно осмыслить проблему, разрешить ее неопределенность и способствовать достижению цели.

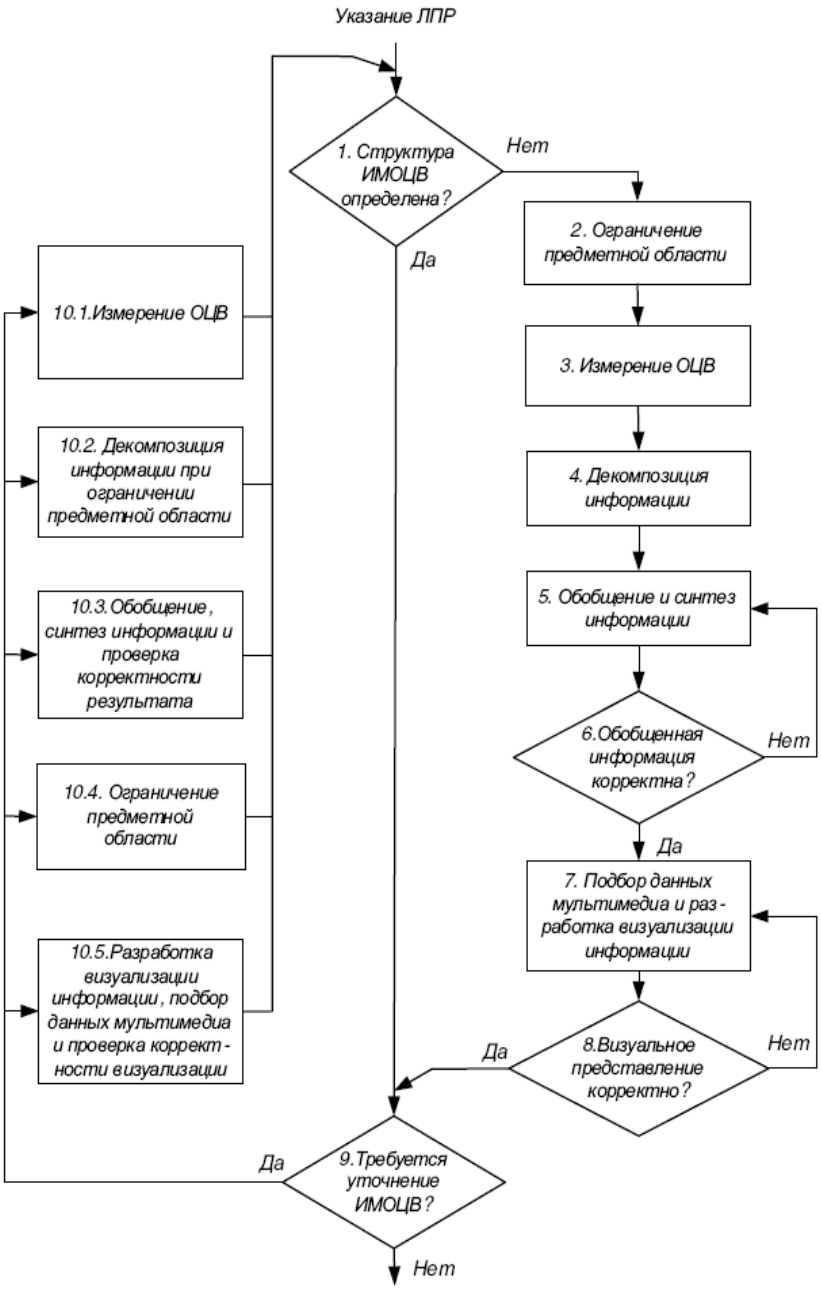
3.2.3. Режимы работы ситуационно-кризисного центра

Как правило, в работе СКЦ выделяются следующие три режима.

3.2.3.1. Режим проблемного мониторинга

Мониторинг объекта целевого воздействия (ОЦВ) и информирование лица, принимающего решение (ЛПР), о достижения ОЦВ заданного состояния. Цель - это желаемое состояние ОЦВ. Решение принимает ЛПР на базе собственного представления о проблеме (знания о цели, личный опыт, интуиция). Далее **представление ЛПР о проблеме рассматривается как информационная модель ОЦВ (ИМОЦВ).** Схема[65] работы:

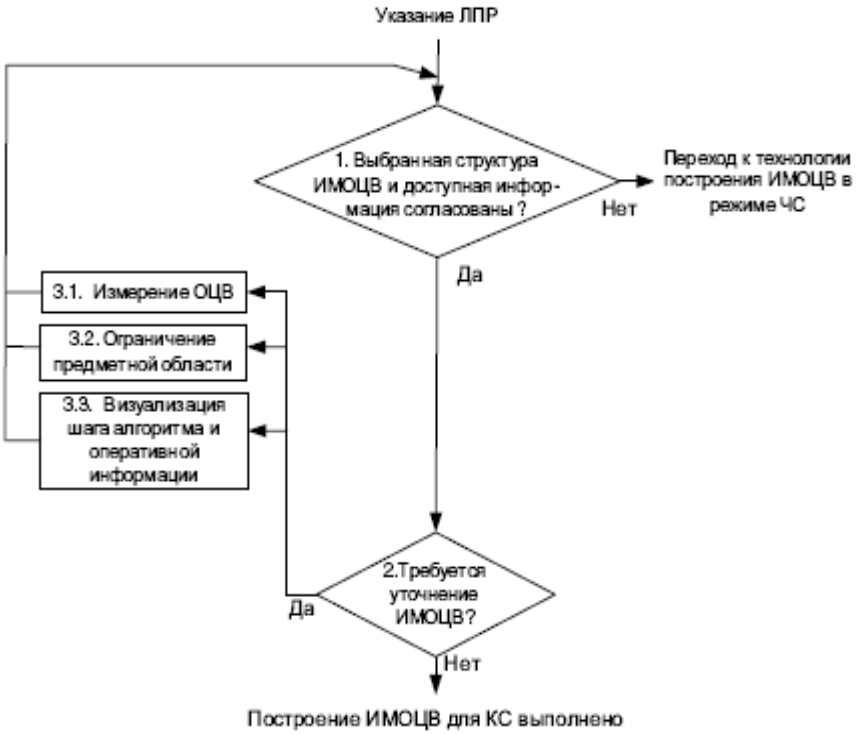
[65] См. Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности. М.: - Издательство «Парад», 2005. С.197.



Построение ИМОЦВ в исследовательском режиме выполнено

3.2.3.2. Режим кризисного реагирования

Режим кризисного реагирования, реализуемый в «он-лайне», когда **на основе прецедентов и накопленной информации о фигурантах ситуации ИМОЦВ содержит готовые алгоритмы решений.** Схема[66] работы для кризисной ситуации (КС):

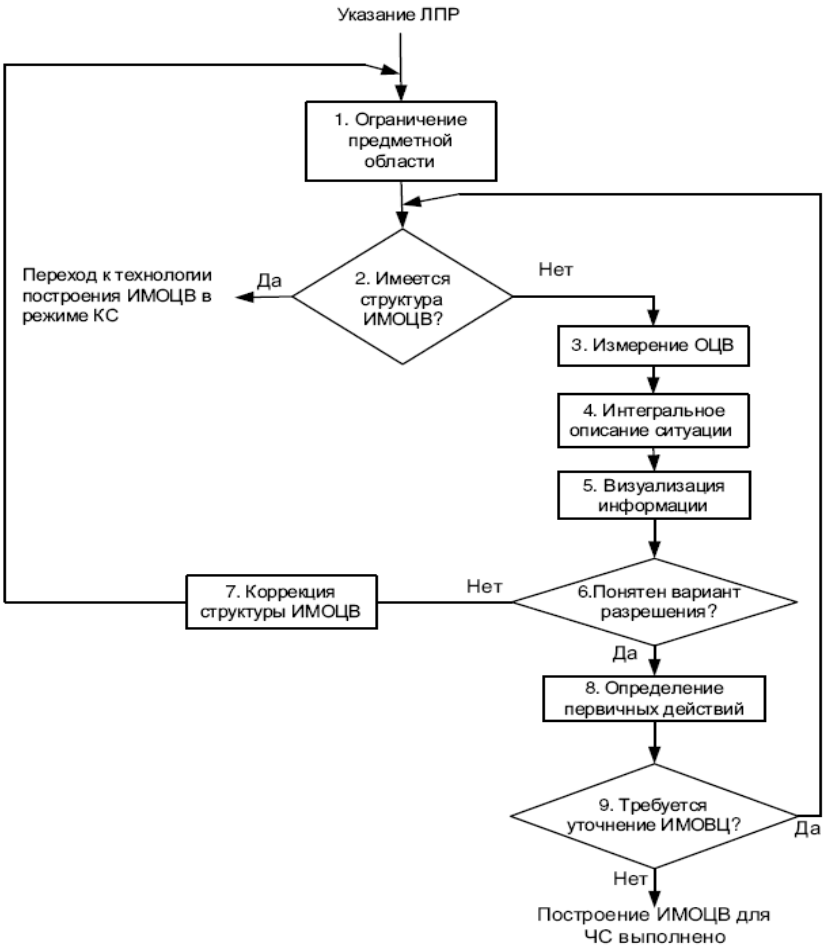


3.2.3.3. Режим чрезвычайной ситуации

Режим чрезвычайной ситуации протекает в «он-лайне». При этом, **в отличие от режима кризисной ситуации, нет знаний о**

[66] Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности. М.: - Издательство «Парад», 2005. С.198.

прецедентах, нет готовых алгоритмов решения и лимит времени весьма ограничен. Схема[67] работы в чрезвычайной ситуации (ЧС):



Таким образом, СКЦ становятся неотъемлемой частью системы обеспечения международной безопасности России, т.к. новые технологии позволяют и принципиально по-новому, инновационно от-

[67] Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности. М.: - Издательство «Парад», 2005. С.199.

слеживать, анализировать, прогнозировать и реагировать на кризисы.

Согласно Стратегии национальной безопасности России до 2020 года (п. 109), угрозы информационной безопасности предотвращаются за счет совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в России, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности.

Концентрация информресурсов в СКЦ делает их мишенью для кибератак. Зарубежный опыт использования СКЦ также доказывает данную дихотомию: с одной стороны, СКЦ - эффективный инструмент исследования проблемы информационной безопасности, в т.ч. международной, а с другой - это объект защиты аккумулируемой в них чувствительной информации.

3.3. Национальный центр управления в кризисных ситуациях МЧС России (НЦУКС)

Национальный центр управления в кризисных ситуациях (НЦУКС) представляет собой территориально-распределенный информационно-управляющий комплекс с периферийными элементами, позволяющими управлять силами, средствами и ресурсами единой госсистемы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС) и гражданской обороны (ГО) в условиях кризисов и чрезвычайных ситуаций (ЧС). В 2008 г. НЦУКС получил статус федерального госучреждения.

Основные задачи центра:

- контроль наличия и готовности сил и средств оперативного реагирования МЧС России к действиям при ЧС мирного и военного характера;
- обеспечение в установленном порядке устойчивого и оперативного управления силами и средствами РСЧС в ходе выполнения мероприятий по предупреждению и ликвидации ЧС мирного и военного времени;
- анализ информации, поступающей от функциональных и территориальных подсистем РСЧС, подготовка на его основе предложений по применению сил и средств РСЧС и, совместно с Всероссийским центром мониторинга и прогнозирования чрезвычайных

ситуаций природного и техногенного характера («Антистихия»), прогнозов возникновения и развития ЧС федерального и межрегионального уровня;

- обеспечение оповещения и информирования органов управления и сил РСЧС о ЧС мирного и военного времени;
- обеспечение взаимодействия со СМИ.

3.3.1. Ситуационный зал оперативной смены НЦУКС

Основные возможности зала:

- отображение информации о ходе ликвидации и предупреждения ЧС, поступающих от территориальных органов МЧС России, федеральных органов исполнительной власти, оперативной группы НЦУКС;
- отображение информации о состоянии гидрометеорологической обстановки в целом по России и по отдельным территориям;
- получение оперативных предупреждений о цунами и других неблагоприятных природных явлениях от Росгидромета;
- отображение обстановки на ядерных и радиационно-опасных объектах России, а также в районах их дислокации по информации поступающей из Росатома;
- отображение информации о силах, средствах, ресурсах;

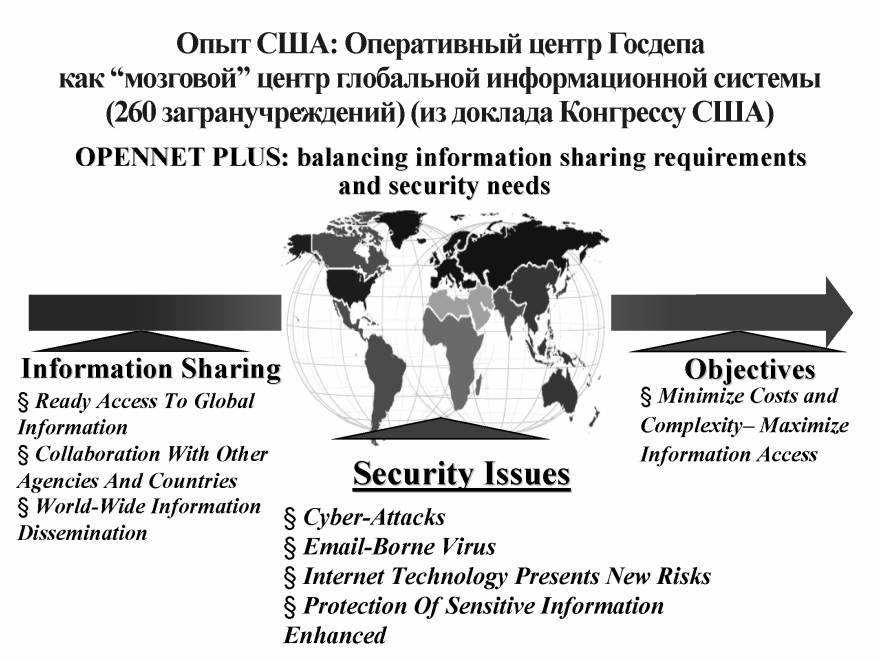
- осуществление контроля за состоянием критически важных для национальной безопасности объектов, включая видеоконтроль;
- осуществление контроля за перемещением особо опасных грузов, конвоев с гуманитарной помощью с использованием систем ГЛОНАСС-GPS.

3.3.2. Ситуационный зал федеральных органов исполнительной власти

Оборудован системой отображения информации на базе мультиэкрана, состоящего из 24-х проекционных модулей с размером экрана каждого 84 дюйма по диагонали. В видеостене использованы проекторы на базе современной DLP технологии формирования изображения. Обеспечивается обработка и отображение видеоинформации от файловых серверов; информации, доступной в ЛВС; комплекта презентационного оборудования с рабочего места оператора; документ-камеры, размещенной на АРМ; оборудования видеоконференцсвязи; компьютеров, установленных в зале и подключенных к компьютерной сети.

3.4. Система кризисного реагирования США

Наиболее амбициозная ведомственная программа развития ИТКС создается в Госдепартаменте США, которая, по сути, поставлена в центр всех информационных систем госорганов.



Из материалов Госдепартамента США, доложенных Комитету Палаты представителей по правительственной реформе (2002 г.), внимания заслуживает следующее:

1. В 260 загранучреждениях США, имеющих представителей из более 30 ведомств, обеспечивается:

- передача по электронной почте конфиденциальной и секретной информации;
- программа безопасного голосового и прямого соединения с публичной федеральной сетью, а также с сетями Минобороны и Госдепа;
- программа радиоподдержки в чрезвычайных ситуациях;
- почтовые и телеграфные услуги, в т.ч. для личной переписки;

- телекоммуникационные и компьютерные услуги (спутниковая связь, провайдеры Интернета, радиосети местной защиты и т.д.);
- телекоммуникационные сети для получения дипломатических сообщений с криптографической защитой и мониторингом безопасности каналов связи;

2. В рамках программы Президента США по внедрению электронной системы управления (стоимость 500 млн.долл. на 2 года):

- введена интегрированная систему передачи сообщений (сбор, обработка, использование, распределение, архивирование и поиск всех государственных сообщений, включая внутренние меморандумы, электронную почту, официальные сообщения, записи и почтовые сообщения);
- выход в Интернет через программу OpenNet Plus 32 тыс.компьютеров сети Госдепа с использованием Системы поиска информации из открытых источников;
- получение доступа к закрытой электронной почте, специальным телеграфным услугам, а также системе «Интелинк» и интернетовской сети отслеживания секретной информации (SIPRNet). Позднее к этой программе подключены все рабочие места (за исключением тех, где обрабатывается несекретная информация и ДСП).

3. Госдеп уже апробировал систему управления информацией (межведомственного взаимодействия), в т.ч. с загранучреждениями в Индии и Мексике.

4. Проблемы межведомственного взаимодействия, в т.ч. безопасности:

- обмен информацией и разведданными, как на горизонтальном уровне, так и на вертикальном (федеральные власти, штаты, местные органы);
- проблемы безопасности связанные с многоуровневым доступом и обменом информации - «несекретной», «чувствительной, но не секретной», «секретной» и «совершенно секретной»;
- консульские услуги - реализация программы, финансируемой Управлением по гражданским делам (УГД), Разведывательно-исследовательским бюро (INR) программы TIPOFF, программы контроля за террористами с использованием разведданных ЦРУ, АНБ и ФБР, Системы консульской проверки в рамках Межведомственной системы пограничного контроля (IBIS), за работу которой отвечают Служба иммиграции и натурализации (ИНС), а также Таможенная служба. ИНС и УГД обмениваются данными в режиме

реального времени, в т.ч. о потерянных или украденных загранпаспортах. ИНС получает данные и фотографии лиц, запросивших неиммиграционные визы во всех своих пунктах въезда. Сотрудник из загранучреждения может иметь доступ к базе данных, где имеется информация по всем выданным и отказанным визам в различных странах мира, о выдаче паспортов и свидетельств о рождении за границей (в рамках системы микрофильмирования паспортных данных). В паспортную службу поступает информация из ФБР и Налоговой службы об умерших и находящихся в розыске, о преступлениях, введены паспортно-визовые документы с биометрическими параметрами владельцев.

3.4.1. Структура Оперативного центра Госдепартамента США

Интеллектуальной вершиной Глобальной информационной системы Госдепа США является Оперативный центр (ок. 100 чел.), созданный в начале 60-х годов для урегулирования Карибского кризиса, политического кризиса в Конго и т.д. Данный орган непосредственно подотчетен исполнительному секретарю Госдепа и отвечает за разработку межведомственной стратегии реагирования на кризисные ситуации в мире.

Ведущее подразделение ОЦ - Группа оперативных дежурных («The Watch») - насчитывает около 45 сотрудников со знанием основных иностранных языков. Дежурства осуществляются в три смены по 6 человек.

Группой в режиме реального времени отслеживаются значимые международные события в глобальном масштабе. На этой базе ежедневно готовятся обзорные доклады и оперативные сводки по «горячим» событиям, а также осуществляется информационное обеспечение зарубежных поездок руководства Госдепа.

В ведении Группы расположен контактный пункт, куда обязаны звонить сотрудники центрального и загранаппарата Госдепа в случаях возникновения угроз их личной безопасности.

Вспомогательным подразделением ОЦ является Штаб содействия урегулированию кризисов (Crisis Management Support), объединяющий порядка 8 человек, из которых 5 - специалисты по региональным проблемам (Африка, Ближний Восток, Восточная Азия и Тихоокеанский регион, Европа и Евразия, Западное полушарие), а также главный инспектор, межведомственный координатор и стажер.

Основная функция Штаба - кризисный мониторинг, экспертные наработки содействия урегулированию кризисных ситуаций, в т.ч. касающихся экстренных мер в случаях нападений на граждан США за рубежом. Ведется обработка срочных шифртелеграмм из загранучреждений для доклада руководству, а в случае необходимости формируются целевые группы (task-force) с возможным участием специалистов из других ведомств, спецслужб и неправительственных организаций.

Штаб также осуществляет чрезвычайное планирование и обучение сотрудников Госдепартамента и ЗУ методам реагирования на кризисы с проведением учений один раз в 2 года (в кризисных регионах - каждый год). Ежегодно такую подготовку проходят до 200 человек.

Оперативный центр Госдепа США поддерживает тесные контакты с аналогичными органами других ведомств: Оперативным центром Министерства внутренней безопасности, Пентагоном, ЦРУ, ФБР и др., а также с «Ситуационной комнатой» Белого дома (кстати, на его сайте дано следующее определение **«Ситуационная комната» (White House Situation Room) - это круглосуточный наблюдательный и сигнальный центр, обеспечивающий Президента, Помощника по национальной безопасности, членов Совета Безопасности текущей разведывательной и открытой информацией для выработки и реализации политики в области национальной безопасности)**. ОЦ проводит «круглые столы» и видеоконференции в открытом и закрытом режимах.

Другим примером СКЦ является Центр стратегической информации и операций ФБР (Strategic Information and Operations Center - SIOC), который сыграл ключевую роль в расследовании событий 11 сентября 2001 г. Центр обеспечивает не только сбор и агрегирование необходимой информации, но и координацию работы по выделенной проблеме различных министерств и ведомств. В частности, по проблеме 11 сентября 2001 г. Центр взаимодействовал с более 500 представителями 32 госагентств.

3.4.2. Информационно-аналитические системы, используемые в ЦРУ и ФБР

ЦРУ уже более 25 лет использует программно-аналитический продукт «**Фэкшенз**», предназначенный для онлайнового информирования Президента об основных угрозах и вызовах.

Его цель - составление с помощью специальных программ прогнозов динамики развития политической и экономической обстановки за рубежом. Эксперты утверждают, что, в частности, с помощью «Фэкшенз» в мае 1991 г. был предсказан августовский путч в СССР. Долгое время методика была засекречена.

Необходимость и значимость системы «Фэкшенз» в настоящее время возросла с учетом возможностей Интернет-технологий (http://www.nationmaster.com).

В 1995 г. к участию в системе «Фэкшенз» были приглашены граждане России. Методика, используемая в системе «Фэкшенз», несложна:

- эксперты-аналитики определяют объект исследования;
- подбирают команду «игроков».

Для определения возможных политических коалиций полученные диаграммы совмещают и строят интегрированный график. Именно таким образом рассчитываются возможные политические союзы.

Один из самых важных результатов изучения полученных диаграмм - это анализ стабильности. Эксперты считают, что **для стабильности необходимо, чтобы руководители государства находились в центре. Это самая устойчивая парадигма**.

В 1994 г. исследования провели в отношении Польши. Они показали, что позиция премьер-министра на диаграмме оказалась с краю и вскоре он покинул пост.

Диаграммы относительно Б.Ельцина в 1992 г. показывали, что оппонирующие коалиции имеют больший вес, и в заключениях экспертов фигурировали опасения развала России или изменение ее курса.

Результаты проведенного в 1995 г. российско-американского исследования к визиту Б.Клинтона в Москву показали, что точка возврата назад для России уже пройдена, даже в случае ухода Б.Ельцина.

Отдел современных ИКТ, входящий в состав управления науки и техники ЦРУ США, продемонстрировал общественности технологии «**извлечения текстовых данных**» («**Text Data Mining**»), используемые для поиска значимой информации в огромной массе документов и в радио- и телепередачах, в т.ч. на иностранных языках.

Поиск ведется как по систематизированным, так и по случайным источникам, причем **объектами поиска являются тексты в печатных изданиях и в цифровом виде, графические изображения, аудиоинформация на 35 языках**. Для отсеивания аудиоин-

формации используется методика «**Oasis**», которая распознает речь и превращает ее в текст. При этом технология позволяет отделять мужские голоса от женских, а также голоса, принадлежащие разным людям, и записывать их в виде диалогов. **Методика позволяет выделять из аудиопотока только те голоса или ту информацию, которая заложена в настройках поиска**.

Другая технология **«Fluent»** позволяет ЦРУ искать информацию в текстах по ключевым словам, причем вводится слово или сочетание на английском языке, которое тут же переводится на целый ряд других языков, и найденная информация из баз данных на разных языках поступает аналитику после автоматического перевода. Программа «Text Data Mining» позволяет автоматически создавать предметные указатели для текстовых документов, а также получать данные по частоте употребления тех или иных слов в документах. **Эти технологии ЦРУ использует сегодня в отслеживании незаконных финансовых операций, наркотрафика, в борьбе против международного терроризма.**

Названными выше технологиями занимается отдел Advanced Information Technology (AIT) Директората науки и технологии ЦРУ. «Мы развиваемся не так быстро, чтобы поспеть за стремительным ростом информационных потоков, стекающихся сюда каждый день, - подчеркнул директор AIT Ларри Ферчайлд (Larry Fairchild) - Мы должны снабжать сотрудников технологией, которая поможет им справиться с гигантскими объемами оперативно обрабатываемых данных»[68].

В плане профессионального использования инструментов Text Mining ЦРУ - далеко не монополист. По прогнозам аналитической компании IDC, спрос на подобные программы существенно возрастет в течение ближайших 4-5 лет. Такие возможности, как экспресс-анализ найденной информации, информационная разведка, формирование и ведение тематических досье с возможностью выявления тенденций и взаимосвязей персон, событий, процессов уже используются рядом крупных структур и будут востребованы в дальнейшем.

[68] http://www.visti.net/~dwl/art/dz/

3.5. Кризисные центры МИД ФРГ и Италии

3.5.1. Центр кризисного реагирования МИД ФРГ

Центр кризисного реагирования (КЦ) МИД ФРГ структурно похож на Оперативный центр Госдепартамента США и также занимает высокое место в иерархии министерства.

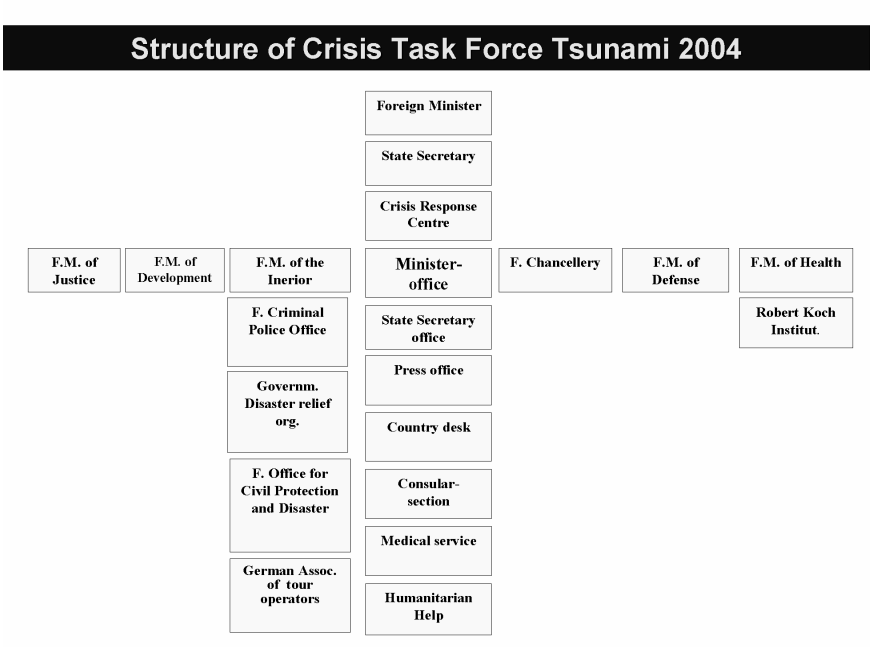
Его основные задачи включают в себя:

- круглосуточный мониторинг сообщений посольств и СМИ;
- обеспечение докладов по ситуациям;
- координацию всех предупреждений;
- раннее предупреждение и инициативные превентивные меры;
- реагирование на кризисы, в т.ч. проведение операций по эвакуации;
- связь с другими правительственными агентствами и частным сектором;
- созыв кризисной рабочей группы;
- оказание помощи гражданам по телефону или электронной почте (советы для выезжающих, информация посольств);
- обеспечение картами и фотографиями со спутников.

Численность Центра кризисного реагирования МИД ФРГ составляет 31 человек, из них: 8 чел. - дежурные Центра, 10 чел. - специалисты, отвечающие за кризисное реагирование, 5 чел. - специалисты, отвечающие за оказание помощи гражданам, 5 чел. - представители силовых ведомств, в т.ч. криминальной полиции, 3 чел. - специалисты по ИКТ.

Характерно, что МИД ФРГ создал группы кризисного реагирования и в загранучреждениях, в задачи которых входит очень широкий круг проблем мониторинга и действий, в т.ч. превентивных.

Наибольшее представление дает организация работы КЦ МИД ФРГ по минимизации потерь после чудовищного цунами в Азии (декабрь, 2004 г.), для чего была четко отработана следующая структура взаимодействия.



В своей работе КЦ МИД ФРГ взаимодействует с КЦ других министерств и ведомств Германии, а также с ситуационным центром Евросоюза.

3.5.2. Кризисный центр МИД Италии

Структура Кризисного центра (КЦ) МИД Италии схожа со структурой КД МИД ФРГ и включает в себя следующие подразделения: отдел реагирования, комната обработки информации, отдел подготовки планов действий в ЧС, отдел анализа региональных рисков, отдел превентивного мер, отдел радио- и спутниковых коммуникаций, телемедицины, видеоконференцсвязи, видеографическая и диспетчерская комнаты, центр анализа GPS, администрация, отдел внутренней безопасности. .

К особенностям данного КЦ можно отнести следующие. Мандат действий КЦ МИД Италии в чрезвычайных ситуациях за границей включает в себя помощь и спасение итальянских граждан, а также защиту итальянских интересов путем:

- анализа степени риска, в т.ч. при взаимодействии с загранучреждениями Италии, представителями спецслужб и мониторинга открытых Интернет-источников СМИ;
- контроля присутствия итальянских граждан в мире, включая итальянских туристов и граждан Италии, проживающих за рубежом (осуществляется в тесном контакте с туроператорами, неправительственными организациями, религиозными деятелями и путем регистрации итальянских граждан на соответствующем Интернет-сайте КЦ);
- составления и подтверждения планов действий в ЧС;
- кризисного управления;
- постоянного взаимодействия с кризисными центрами стран Евросоюза.

3.6. Международный ситуационный центр (МСЦ) анализа агрессивных воздействий на окружающую среду (РАГС - Университет Пармы)

Среди новых угроз глобальной безопасности особое место занимает вредоносное антропогенное воздействие на окружающую среду. При этом кризисные ситуации (КС) могут возникнуть как в результате непреднамеренных техногенных катастроф, так и в результате злого умысла (например, теракта). **Количество и масштабность преднамеренных угроз окружающей среде со стороны террористов неуклонно растет, а многие производственные сооружения и объекты инфраструктуры являются весьма уязвимыми: системы энерго- и водоснабжения, промышленные предприятия, сельские хозяйства, склады с химическими удобрениями, городская инфраструктура и т.д**.[69]

КС крупного масштаба наносят окружающей среде ущерб, который редко ограничивается пределами одной страны. Для противодействия подобным угрозам требуется консолидация усилий ряда государств. В силу этого и возник проект создания МСЦ для анализа агрессивных воздействий на окружающую среду.

МСЦ как контрмера против экотерроризма создается по проекту SITCEN в рамках Программы НАТО «Наука ради мира и безопасности». Основными исполнителями проекта определены Университет Пармы - Consortium for Environmental Sciences (Италия) и Академия геополитических проблем. Прототип МСЦ поручено создать РАГС при Президенте РФ[70].

Заметим, что наметилась некоторая путаница в терминологии: «экотерроризм» чаще употребляется в другом смысле - как «применение или угроза применения насилия криминального характера против законопослушных граждан или их собственности организациями, считающими себя защитниками окружающей среды и действующими по политическим или экологическим мотивам». По оценке ФБР, общий ущерб от экотерроризма превысил $100 млн. Примерами экотерроризма являются:

---

[69] Нельсон Мармироли, Владимир Кривилев, Елена Маестри, Марта Мармироли. Международный ситуационный центр как контрмера против экотерроризма // Ситуационные центры и современные информационно – аналитические технологии поддержки принятия решений: Материалы научно-практической конференции, состоявшейся в РАГС 7-9 апреля 2008 года./ Под общ. ред. А.Н.Данчула. - М.: Изд-во РАГС, 2009

[70] С 2011 г. - РАНХИГС

- диверсии на линиях электропередач;
- поджоги станций лесной службы, деревоперерабатывающих предприятий, фирм по переработке мяса, горнолыжных курортов;
- нападения на звероферм и научные лаборатории, где медицинские препараты испытывают на животных.

В настоящем параграфе рассматривается возможность использования двух разработанных информационно-аналитических систем в интересах поддержки принятия решений в МСЦ.

3.6.1. Мониторинговая информационно-аналитическая система «Ангара»

Важное место в программном обеспечении ситцентров занимают мониторинговые информационно-аналитические системы (ИАС), которые позволяют отслеживать исследуемый процесс в близком к реальному времени, что для таких динамичных процессов, как КС (особенно при терактах), является совершенно необходимым.

Практика показала, что для проблемного мониторинга о различных пространственно-распределенных событиях (в т.ч. терактах) удобно использовать электронные карты. При этом применение специальных ГИС из-за сложности их эксплуатации не всегда оправдано.

К мониторинговым ИАС МСЦ предъявляются следующие требования[71]:

- простота общения с ИАС пользователей, зачастую не имеющих специальной подготовки в области ИКТ;
- снижение информационной нагрузки на конечного пользователя, предоставляя только оперативно значимую для него информацию;
- простота технической эксплуатации системы;
- автоматизация отображения на электронной карте связанных с заданными типами КС пространственно-распределенных событий;
- реализация основных аналитических функций.

[71] Кретов В.С., Котов Н.М. Информационно-аналитическая система мониторинга последствий агрессивных воздействий на окружающую среду для Международного ситуационного центра // Тезисы докладов на международной конференции «Безопасность окружающей среды и экотерроризм» / Москва, Академия геополитических проблем, 27-29 апреля 2010 г.

Всем этим требованиям удовлетворяет отечественная ИАС «Ангара»[72]:

1. **Снижение информационной нагрузки на конечного пользователя** благодаря:

а) наличию различных режимов поиска информации в базах данных системы:

- поиск с уточнением тематики;
- поиск с автоматическим формированием рефератов сообщений, источников и тематик сообщений;
- поиск с использованием электронной карты;

б) наглядной графической репрезентации результатов аналитических расчетов;

в) «скачиванию» информации из сети Интернет не только по адресам, но и по заданным пользователем тематикам;

г) дифференцированному распределению результатов «скачивания» информации пользователям по их профилям.

2. **Простота общения с ИАС «Ангара» конечных пользователей** на основе «дружественного» интерфейса» за счет сформированных разработчиком для данной предметной области моделей информационно-поисковых запросов.

3. **Обеспечение возможности автоматической «привязки» событий, выделенных из входных информационных сообщений, к географическим объектам** на электронных картах. При этом электронная карта служит также в качестве графического интерфейса, позволяя получить атрибутивную информацию, связанную с географическим объектом.

4. **Поддержка основных механизмов аналитических исследований** (контент-анализ и ивент-анализ информации, автоматический мониторинг событий, связанных с заданными пользователями объектами и/или персонами) для оперативного анализа информационных материалов.

5. **Ведение картотек различных объектов** («проблемы», «государства», «международные организации», «персоны» и т.п.), что позволяет реализовать различные прикладные технологии ИАС «Ангара».

6. **Простота технической эксплуатации системы** за счет автоматизации процесса ввода информации в базы данных с ее автоматической рубрикацией. «Ангара» позволяет работать на автоном-

[72] Кретов В.С., Котов Н.М. Информационно-аналитическая система «Ангара» // Ситуационные центры и современные информационно-аналитические технологии поддержки принятия решений: Материалы научно-практической конференции в РАГС 7-9 апреля 2008 года./ Под общ.ред. А.Н.Данчула. - М.: Изд-во РАГС, 2009

ном компьютере, в локальных сетях и сети Интернет в среде Windows 98, NT WorkStation, NT Server, Windows 2000 (WorkStation, Server), Windows XP.

7. **Высокие адаптационные возможности ИАС «Ангара»** обусловлены наличием механизма автоматизированного формирования и коррекции моделей информационно-поисковых запросов, настраивающих ее на различные предметные области.

3.6.2. Результаты апробации ИАС «Ангара»

3.6.2.1. Поиск с уточнением тематики («разлив нефти»)

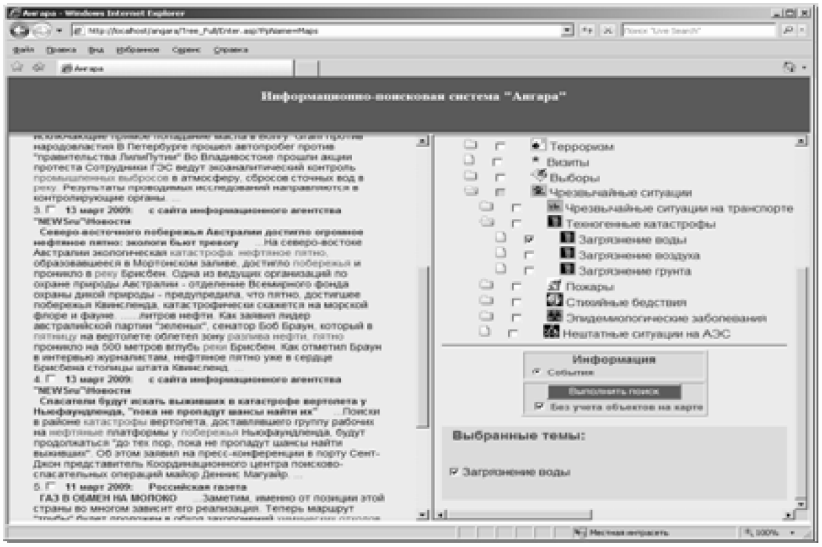


Рис. 3.1. Инициация поиска

```
[.(токсичнЪ  ртутЪ [тяжелые металлы] [(промышленЪ бытовыЪ
химическЪ радиактивнЪ радиационЪ ) (сбросЪ выбросЪ стокЪ
отходЪ загрязненЪ)]) (!воды водоемЪ !рек !реки !реку !река !озер
!озеро !озере !море !моря !океан !океана рыбЪ)]+[.нефтЪ (пятнЪ
пленкЪ концентрацЪ !ПДК загрязненЪ выльютЪ разливЪ выльетЪ
катастрофЪ аварiЪ  ) (!воды водоемЪ !водах !рек !реки !реку !река
!озер !озеро !озере !море !моря !океан !океана рыбЪ танкерЪ
пляжЪ побережЪ)] [.(токсичнЪ вредныЪ опасныЪ  ртутЪ [тяжелые
металлы] автотранспортЪ промышленЪ бытовыЪ химическЪ
радиактивнЪ радиационЪ !ПДК) (сбросЪ утечкЪ выбросЪ
загрязненЪ) (воздухЪ атмосферЪ воздушнЪ)] [.(токсичнЪ  ртутЪ
[тяжелые металлы] [(промышленЪ  бытовыЪ химическЪ
радиактивнЪ радиационЪ ) (сбросЪ выбросЪ стокЪ отходЪ
загрязненЪ)]) (земельЪ землЪ почвЪ грунтЪ)]+[.нефтЪ (пятнЪ
пленкЪ концентрацЪ !ПДК загрязненЪ выльютЪ разливЪ выльетЪ
катастрофЪ аварiЪ  ) (земельЪ землЪ почвЪ грунтЪ)]
```

Рис. 3.2. Вид поискового запроса (строится автоматически!)

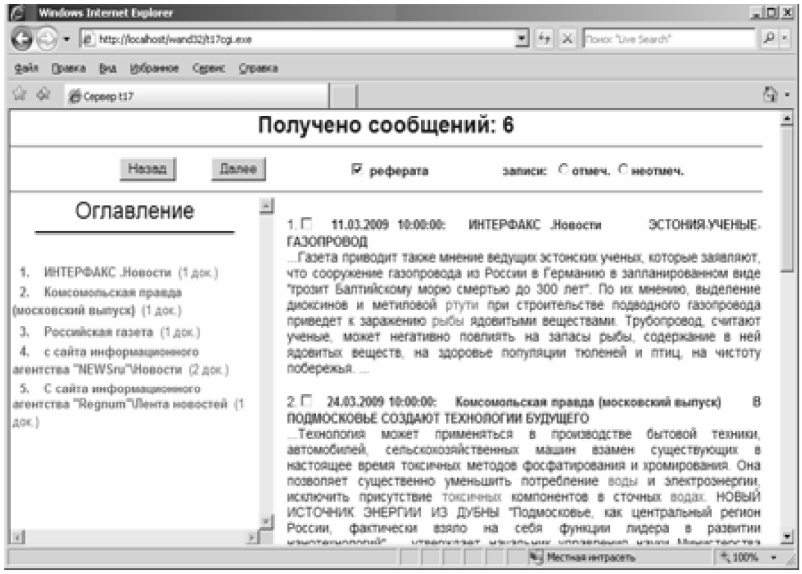


Рис. 3.3. Результаты поиска
с автоматическим формированием источников

Справка о чрезвычайной ситуации в районе Керченского пролива

1. Дата, место, время аварии - 11.11. 2007 г., Керченский пролив и акватория Черного моря (Краснодарский край, Темрюкский район).
2. Наименование нефтепродукта - мазут.
3. Общее количество нефтепродукта - 8777 т.
4. Количество вылившегося нефтепродукта - 2000 т.
5. Площадь загрязнения морской акватории.

По данным авиаразведки на 16.11.2007 г., площадь нефтяных пятен, которые удалось обнаружить визуально, составляла ориентировочно 7,5-10 млн.кв.м. (по информации Главного управления МЧС России по Краснодарскому краю). На 21.11.2007 г. эта информация не подтвердилась.

6. Протяженность загрязненной береговой линии.

По данным Росприроднадзора, загрязнено 113 км. береговой линии, наблюдается повторное загрязнение. Протяженность сильнозагрязненной береговой линии составляет около 49 км.

7. Глубина загрязнения береговой линии - до 3 м.

3.6.2.2. Мониторинг кризисной ситуации «разлив нефти» с использованием электронной карты

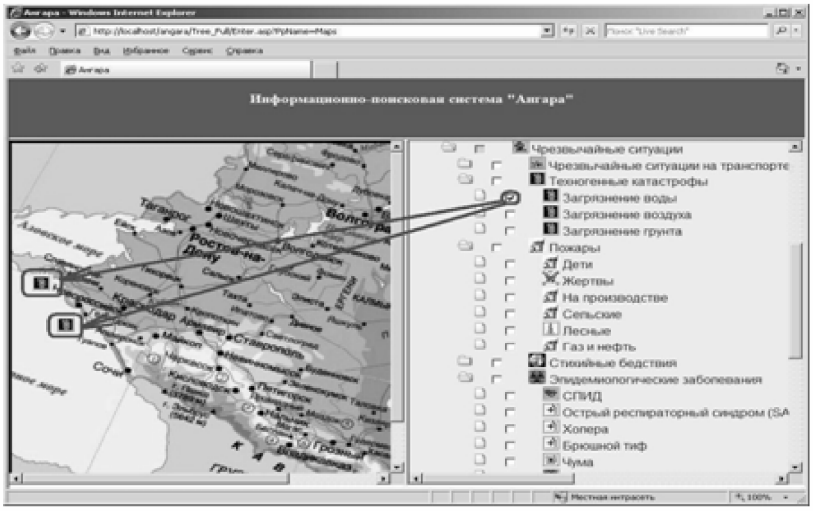


Рис. 3.4. Результат автоматического нанесения на электронную карту информации о разливах нефти в Черном море в период 2007-2008 гг.

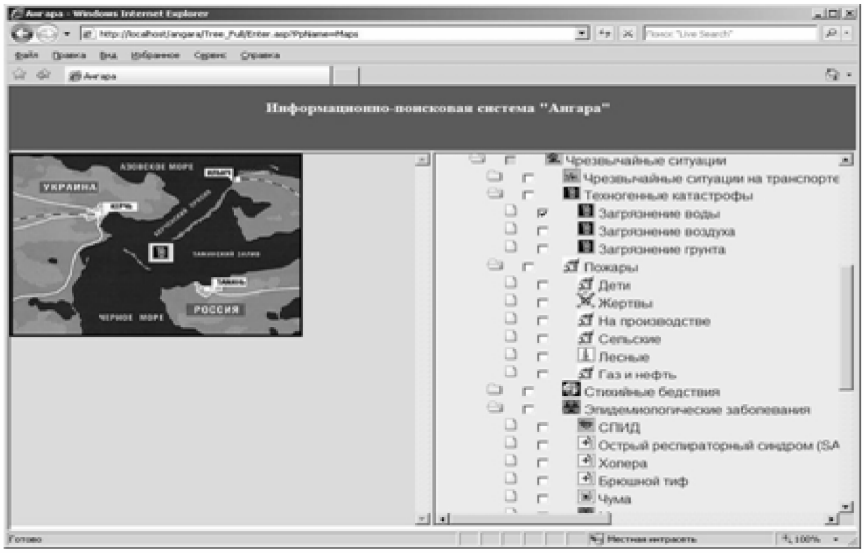


Рис. 3.5. Автоматическое нанесение на ЭК информации о разливе нефти в Керченском проливе в августе 2007 г.

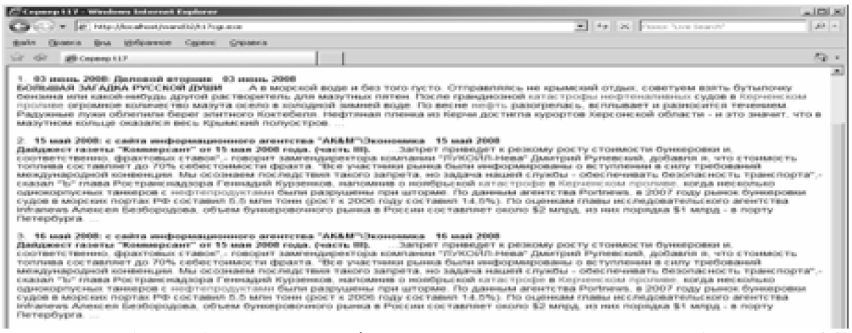


Рис. 3.6. Атрибутивная информация, связанная с выбранной КС (разлив нефти) и географическим объектом (Керченский пролив) (фрагмент)

3.6.3. Выбор системы поддержки принятия решений (СППР) в МСЦ

К системе поддержки принятия решений (СППР) в МСЦ предъявляются следующие требования[73]:

1) работа в условиях жесткого лимита времени, отведенного на оценку обстановки и принятие решений в КС;

2) высокие требования к качеству принимаемых с использованием СППР решений;

3) удобство взаимодействия с СППР с пользователями, не имеющими специальной подготовки в области информационных технологий;

4) работа с неполной, слабо формализованной и нечеткой исходной информации о КС;

5) возможность накопления знаний об имевших место КС с целью использования при принятии решений имеющегося опыта разрешения кризисных ситуаций;

6) удобство работы с большими массивами данных;

7) возможность консолидировать разнородную информацию о КС в различных форматах и организовать высокоскоростной доступ к ней.

Существующие СППР не в полной мере соответствуют указанным требованиям, что не позволяет использовать здесь известные подходы.

Данный фактор вызвал необходимость разработки новой СППР - Экспертной системы поддержки принятия решений в кризисных ситуациях (ЭС ПРКС), отвечающей всем перечисленным выше требованиям.

3.6.3.1. Экспертная система поддержки принятия решений в кризисных ситуациях (ЭС ПРКС)

Работа ЭС ПРКС основана на автоматической классификации текущей кризисной ситуации в условиях неполной и нечеткой входной информации и формировании рекомендаций по преодолению кризисной ситуации на основании действующих нормативных

[73] Кретов В.С., Лебедев И.С. Система поддержки принятия решений в чрезвычайных ситуациях на потенциально опасных и критически важных объектах // Ситуационные центры и современные информационно-аналитические технологии поддержки принятия решений. Материалы научно-практической конференции, состоявшейся в РАГС 7-9 апреля 2008 г. / Под общ. ред. А.Н.Данчула.-М.: Изд-во РАГС, 2009.

документов в соответствии с распознанным классом кризисной ситуации.

ЭС ПРКС имеет возможность:

1. **Автоматизированного обучения системы** с использованием отклассифицированной экспертом обучающей матрицы прецедентов кризисных ситуаций и **автоматической классификации текущей кризисной ситуации** с использованием имеющихся классификаций.

2. Работы со **слабо формализованной нечеткой информацией.** В ЭС ПРКС реализован математический аппарат нечеткой логики и созданы элементы управления, позволяющие пользователю задать уровень достоверности значений в описании кризисных ситуаций.

3. В пользовательском интерфейсе **отображать большой объем информации без информационного «шума»**, для чего реализованы «полупрозрачные» экранные формы и подкрашивание элементов обучающей матрицы с разным уровнем достоверности в разные цвета с целью концентрации внимания пользователя на основной проблеме.

4. Взаимодействия с **другими элементами «дружественного» интерфейса** (выпадающие меню, графическая репрезентация результатов расчетов - диаграммы, деревья решений в графической форме, представление деревьев решений на естественном языке, выдача справок пользователю).

5. **Проведения анализа статистических показателей качества дерева решений встроенными средствами**, позволяющего определить, в каком направлении следует повышать качество базы знаний, в кризисных ситуациях какого класса в обучающей выборке меньше всего знаний, какие атрибуты характерны для того или иного класса кризисных ситуаций и т.п. Все это **выявляет дополнительные закономерности в базе знаний**.

3.6.3.2. Результаты апробации ЭС ПРКС

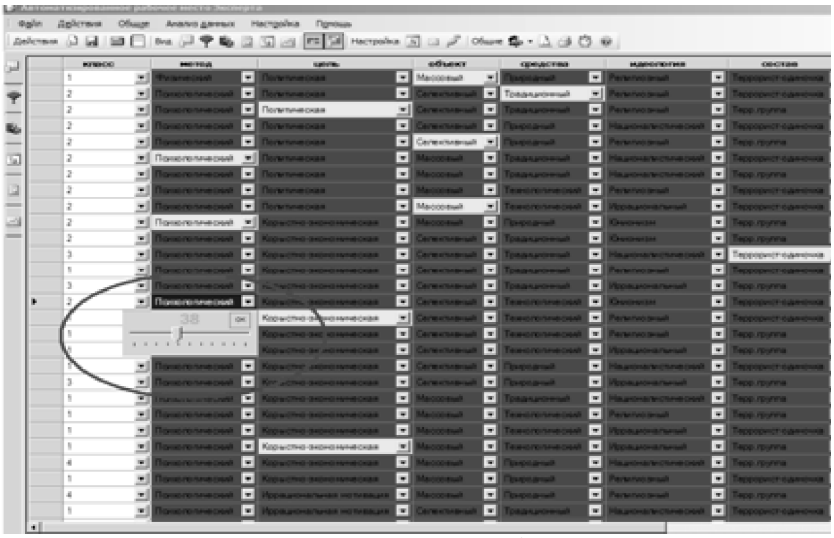


Рис. 3.7. Ввод и редактирование обучающей матрицы

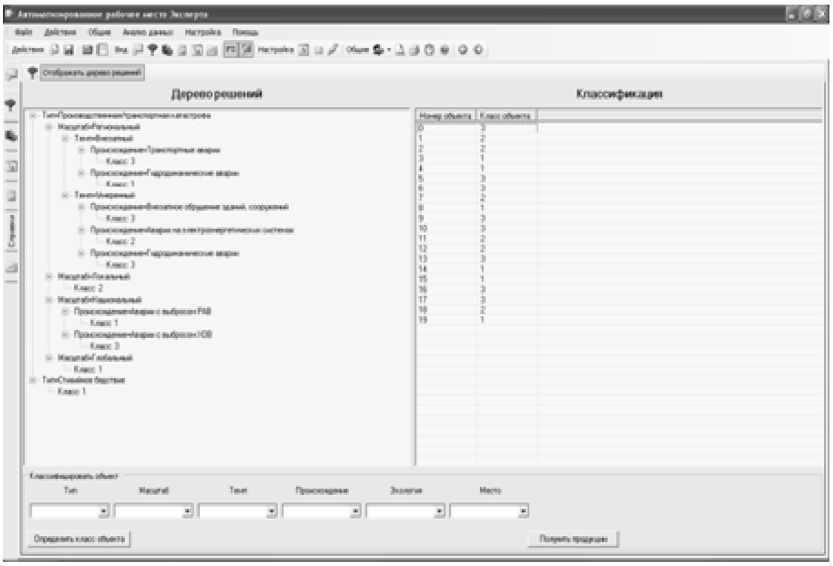


Рис. 3.8. Построенное автоматически дерево решений

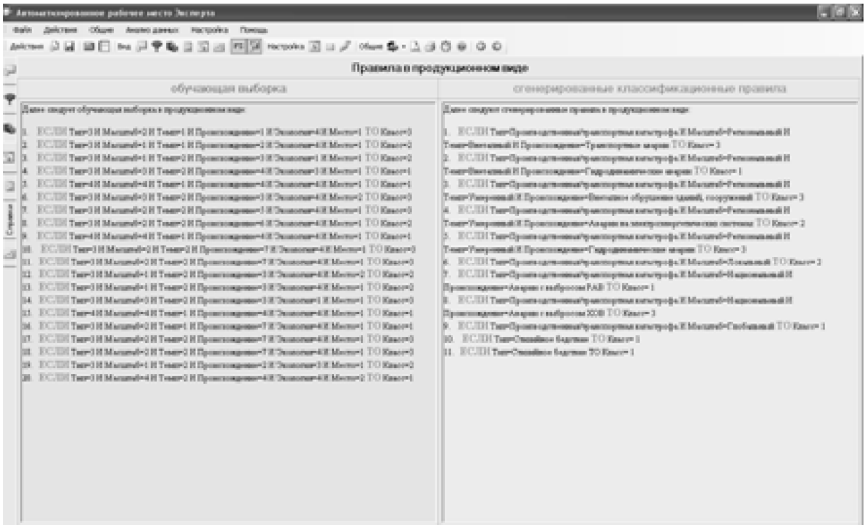


Рис. 3.9. Обучающая выборка и сгенерированные правила классификации в виде продукций

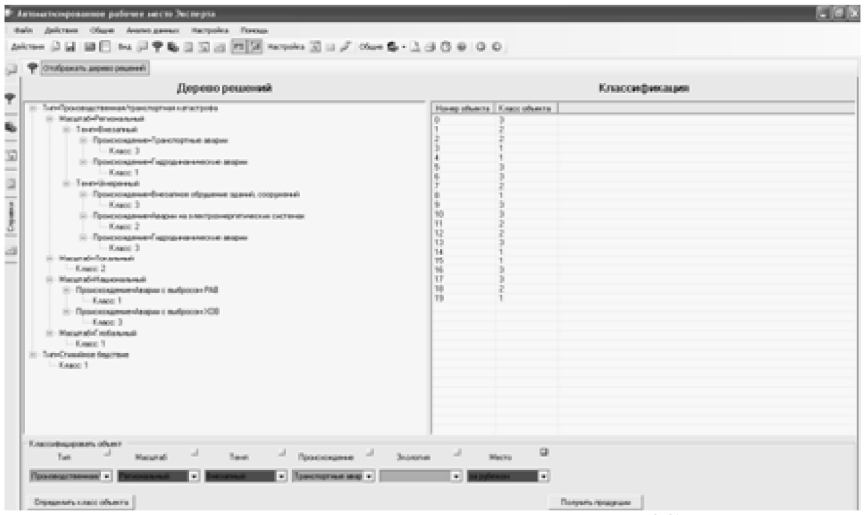


Рис. 3.10. Ввод описания текущей КС

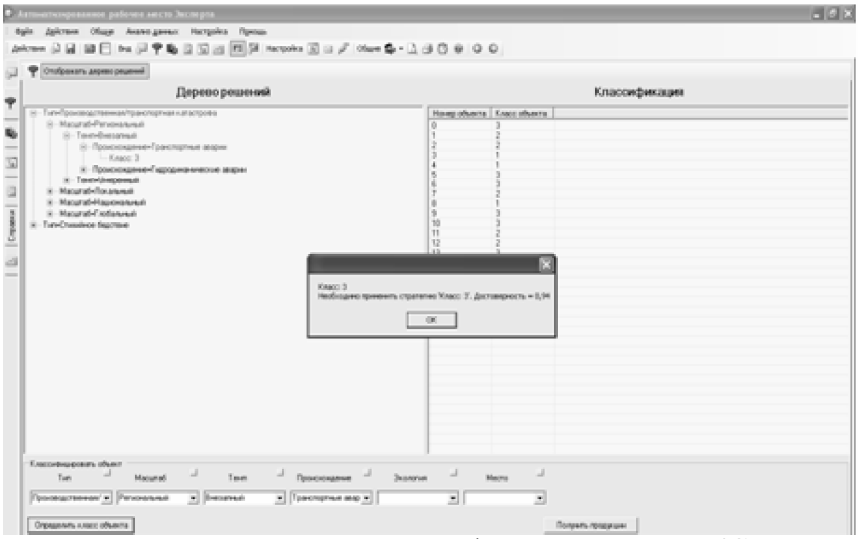


Рис. 3.11. Результат классификации текущей КС

Таким образом, мониторинговые системы ИАС «Ангара» и ЭС ПРКС удовлетворяют требованиям для использования в прототипе МСЦ для анализа последствий агрессивных воздействий на окружающую среду.

3.7. Геоинформационные системы в конфликтологии

3.7.1. Синопсис геоинформационных систем (ГИС). Сравнительный анализ функциональных, экономических и специальных возможностей ГИС

Проведение проблемного мониторинга и кризисного реагирования на современном этапе характеризуется высокой скоростью развития событий. В свою очередь, все события имеют конкретную «взаимоувязку» с любой из географических точек земного шара и, как правило, развиваются на информационно избыточном поле. Эти обстоятельства обуславливают потребность в использовании конфликтологами качественно нового инструментария, в т.ч. ГИС.

Их отличительной особенностью является возможность «привязки» практически неограниченного количества поисковой аналитически обработанной информации к географической основе. Не случайно в зарубежной и отечественной практике по организации

СКЦ в их структуре обязательно присутствует блок картографии и геоинформсистем.

Согласно одному из определений, **ГИС - это автоматизированная информационная система, предназначенная для обработки пространственно-временных данных, основой интеграции которых служит географическая информация.**

В настоящее время более 100 организаций и фирм предлагают системы для создания ГИС-технологий. При этом базой создания ГИС служат так называемые инструментальные пакеты, представляющие программно-технологические комплексы. Они работают с базами данных двух типов - графическими и атрибутивными.

Графическая (пространственная) информация векторных ГИС описывает расположение и очертания объектов. **Атрибутивная** (тематическая) информация содержит описание количественных и качественных характеристик объектов и связей между ними.

В ГИС существуют различные внутренние и обменные форматы графических данных (информации), часть из которых стала практически стандартами. В России для обмена информацией, наряду с другими форматами, используются форматы F1M (Федеральная служба геодезии и картографии) и SXF (военно-топографическое управление ГШ ВС РФ).

Рассмотрим отличительные особенности некоторых ГИС.

3.7.1.1. Особенности семейства программного обеспечения ESRI «ArcGIS» для подготовки данных к выполнению анализа и представления результатов

Программное обеспечение (ПО) «ArcGIS» фирмы ESRI представляет собой интегрированную среду для создания и поддержки ГИС на разных уровнях: для одного и многих пользователей, на настольных компьютерах, серверах, в сети Интернет. Семейство продуктов «ArcGIS» включает структуру профессиональных ГИС-приложений, встраиваемые компоненты для разработки собственных ГИС-приложений, серверные ГИС и др.

Программные средства ArcGIS позволяют найти, просмотреть, документировать и сформировать географические данные и создать сложные базы геоданных для их хранения (приложения ArcMap и ArcCatalog соответственно, рис. 3.12.).

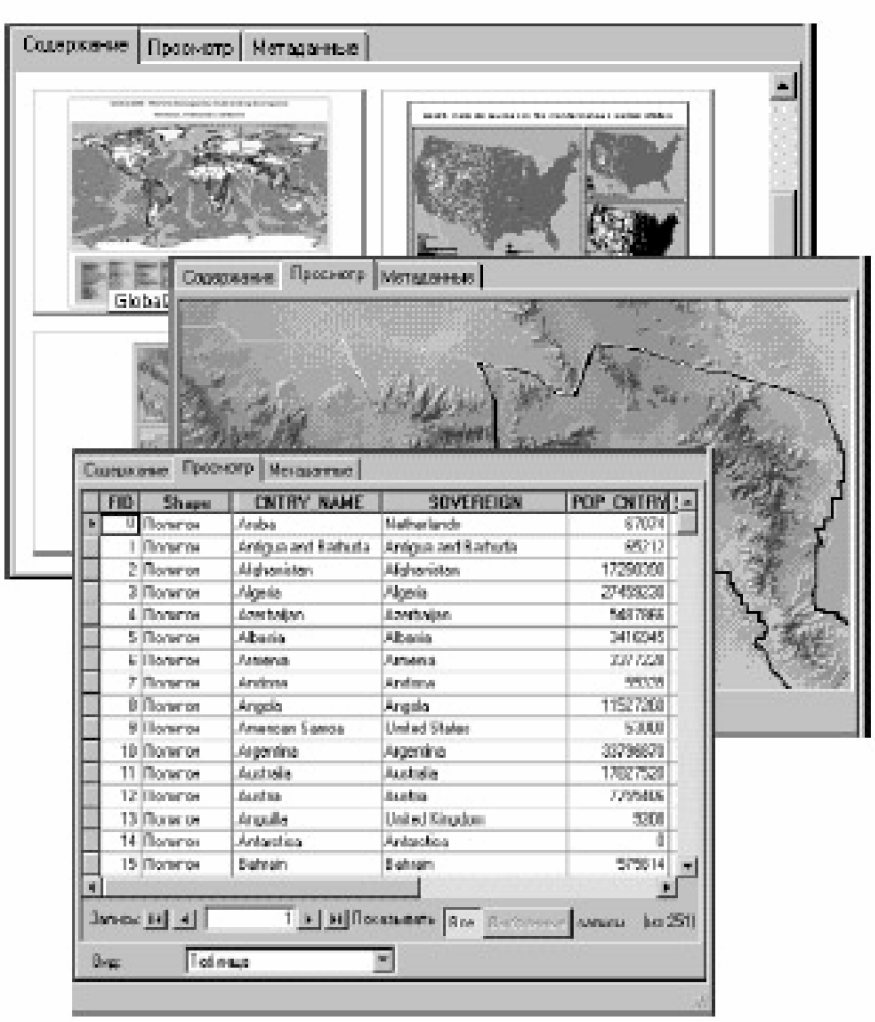


Рис. 3.12. Настройка и оперирование
из удаленных систем баз данных

Прикрепление атрибутивной информации к картографической основе осуществляется через организацию гиперссылок на тематическую информацию. Рисунки 3.13-3.15. иллюстрируют данный процесс.

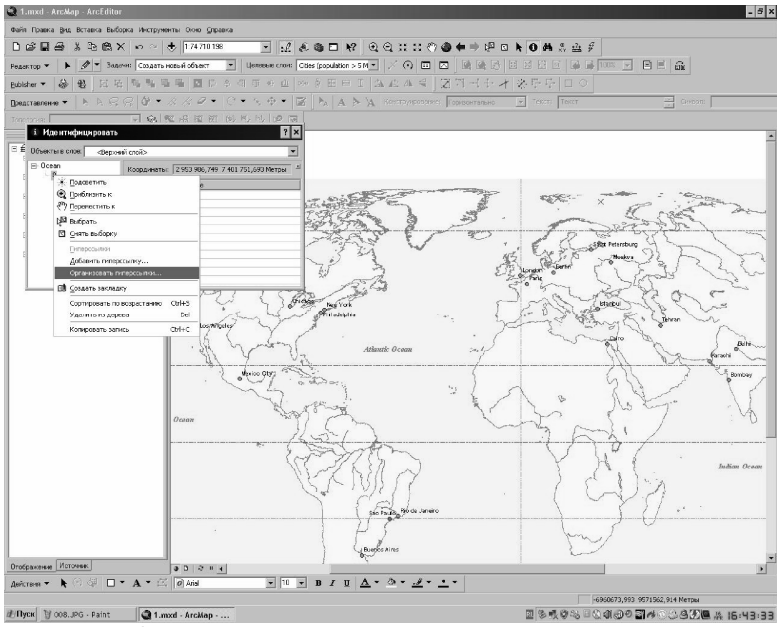


Рис. 3.13. Организация гиперссылки в приложении ArcMap

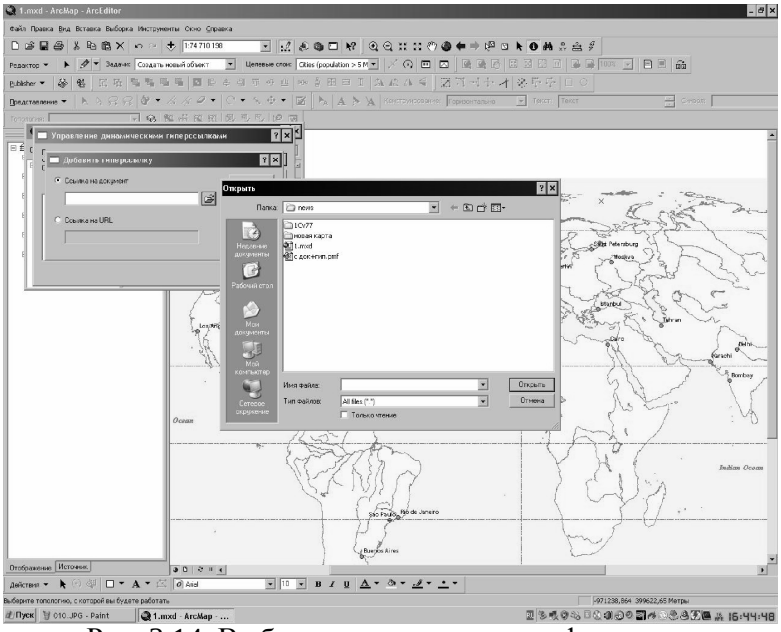


Рис. 3.14. Выбор и прикрепление информации
к географической основе

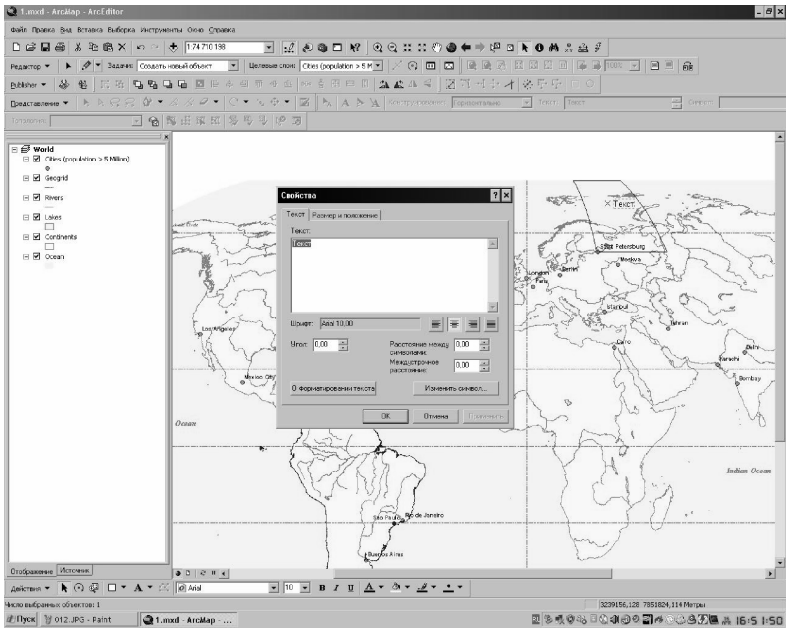


Рис. 3.15. Установка наименования ссылки
к атрибутивной информации

Следует отметить, что универсальность данной ГИС ограничивается ее повышенными требованиями к средствам вычислительной техники, отсюда - большие затраты времени на обработку данных и ответы на запросы.

3.7.1.2. Специфика установки атрибутивной объектовой привязки баз данных в ГИС INTERGRAPH «GeoMedia Professional»

ГИС «GeoMedia Professional» (фирма «Intergraph», США) является универсальной полнофункциональной системой, позволяющей без конвертации подключаться и работать с геоинформационными базами данных большинства форматов, эффективно интегрировать геоданные в единую информсистему от одного оператора до всей организации.

Областью применения является ввод, сопровождение и ведение (администрирование) геоинформационых баз данных, ГИС-анализ, тематическое картографирование и другие функции любого уровня для различных областей использования. **Ресурсы ГИС «GeoMedia**

Professional» позволяют наиболее оптимально проводить кризисное прогнозирование во внешнеполитической деятельности.

Организация атрибутивной объектовой привязки информации в ГИС «GeoMedia Professional» осуществляется посредствам баз данных Warehouse. Причем данный инструмент интегрирован в основную оболочку операторского модуля. Проиллюстрируем процедуру добавления актуальной информации в базу данных и прикрепления ее к картографической основе на рисунках 3.16 - 3.20.

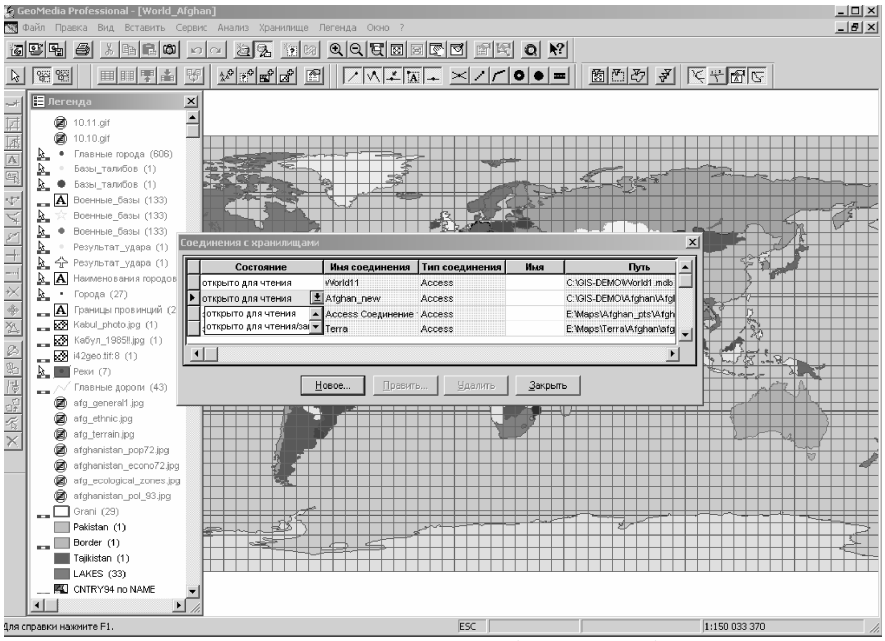


Рис. 3.16. Процесс открытия необходимой базы данных для редактирования

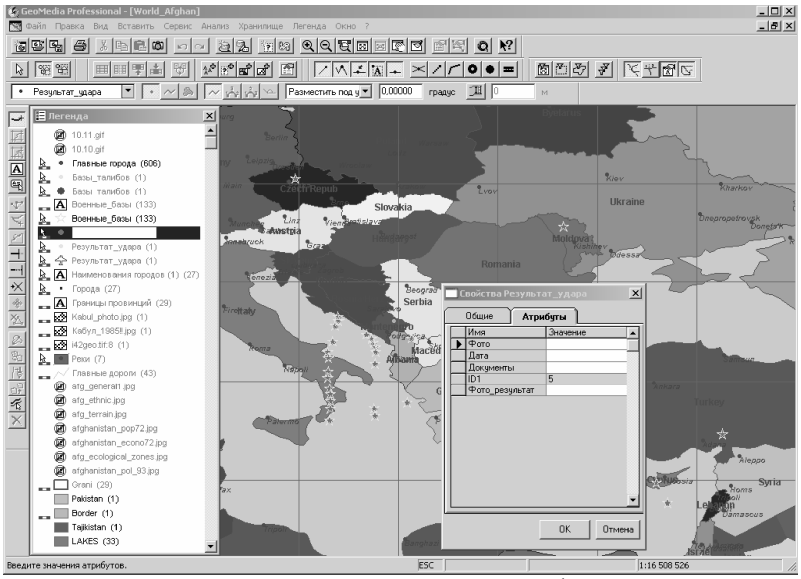


Рис. 3.17. Постановка точки на картографической основе и добавление контекстовых свойств к точке, в т.ч. ссылок на внешние документы

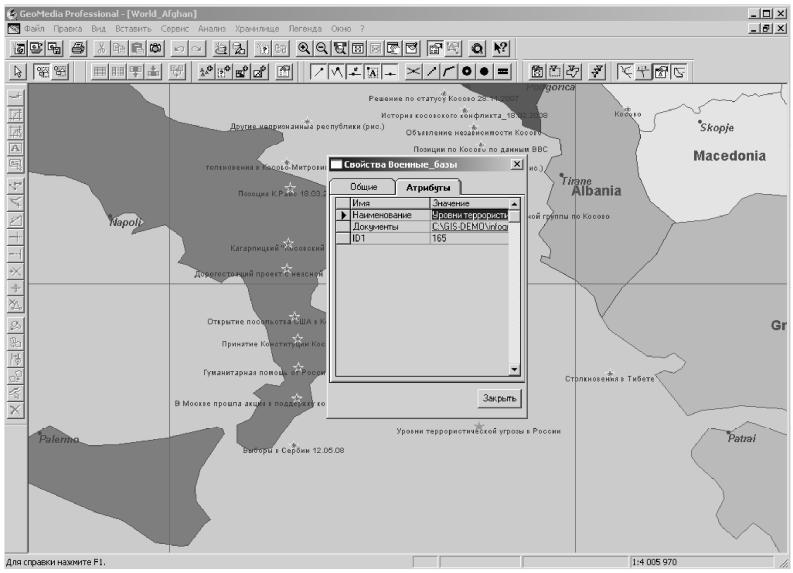


Рис. 3.18. Пример доступа к ссылкам атрибутивной информации в проблемной точке

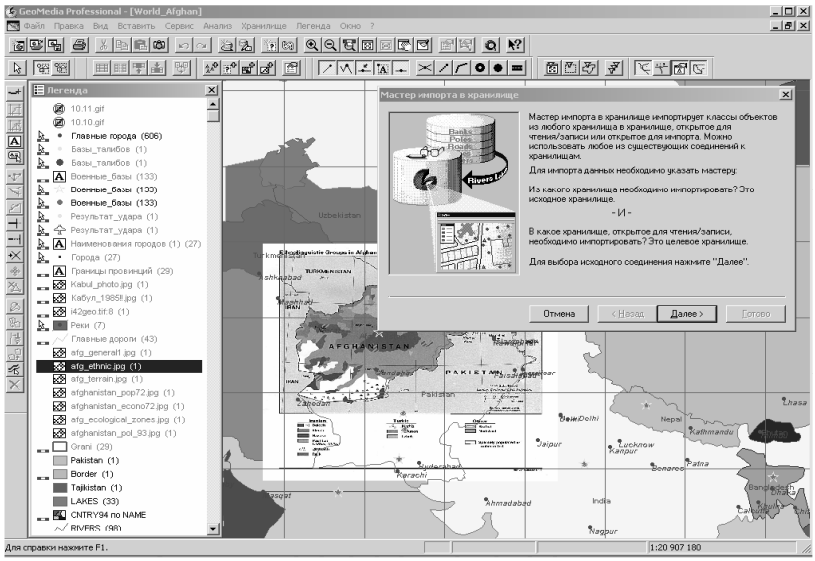


Рис. 3.19. Задействована функция импорта данных в хранилище Warehouse для передачи данных к внешним потребителям информации

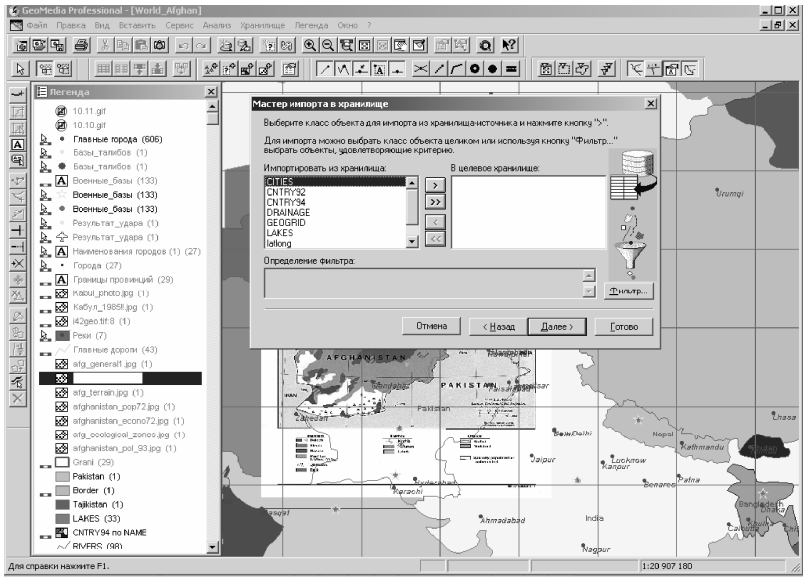


Рис. 3.20. Присутствует возможность импортировать как отдельные позиции данных легенды карты, так и всю карту целиком

Достоинством ГИС «GeoMedia Professional» является полная интегрируемость в операционную среду, что делает ее доступной для всех приложений, а также наличие дополнительных прикладных модулей.

ГИС обладает интуитивно понятным для пользователя интерфейсом, что позволяет одинаково успешно использовать ее как профессионалам, так и новичкам в геоинформатике. Управление хранением в базах данных географической информации и ее администрирование осуществляется напрямую из программы. Наличие возможности без помощи внешних приложений создавать новые данные при помощи «разумных» инструментов существенно повышает качество и скорость ввода географической информации.

К незначительным недостаткам данной ГИС можно отнести относительную высокую стоимость программного продукта и необходимость русифицирования интерфейса.

3.7.1.3. Основные параметры ГИС «Карта 2005» КБ «Панорама» и реализация клиент-серверных приложений

Профессиональная «ГИС Карта 2005» (КБ «Панорама») - универсальная система, имеющая средства создания и редактирования электронных карт, выполнения различных измерений и расчетов, построения 3D моделей, обработки растровых данных, средства подготовки графических документов в электронном и печатном виде, а также инструментальные средства для работы с базами данных.

Система многофункциональна и полностью открыта для решения широкого круга задач, использующих геоинформацию. Преимуществом является наличие отечественного разработчика как самого программного обеспечения, так и картографических основ, а также поддержка стандартных систем классификации, кодирования объектов и их характеристик в соответствии с требованиями Роскартографии, Топографической Службы ВС РФ и других федеральных служб.

Условиями, ограничивающими применение «ГИС Карта 2005», могут считаться трудности при совместимости картографических основ с другими ГИС.

Наиболее востребованной функцией ГИС «Карта 2005» с точки зрения проведения анализа фаз конфликта является тематическое картографирование. Под тематическим картографированием понимается формирование графических изображений, наглядно иллюст-

рирующих соотношение значений выбранной характеристики для отдельных объектов электронной карты. Вместе с тем, существует возможность удаленного доступа к базам данных и электронным картам (клиент-серверное приложение GIS Webserver). Наличие у пользователя выхода в сеть Интернет предоставляет возможность просматривать топографические карты и таблицы базы данных, выполнять поиск и выбор объектов карты, редактировать семантику объектов, масштабировать и перемещать карту, изменять состав изображения и др.

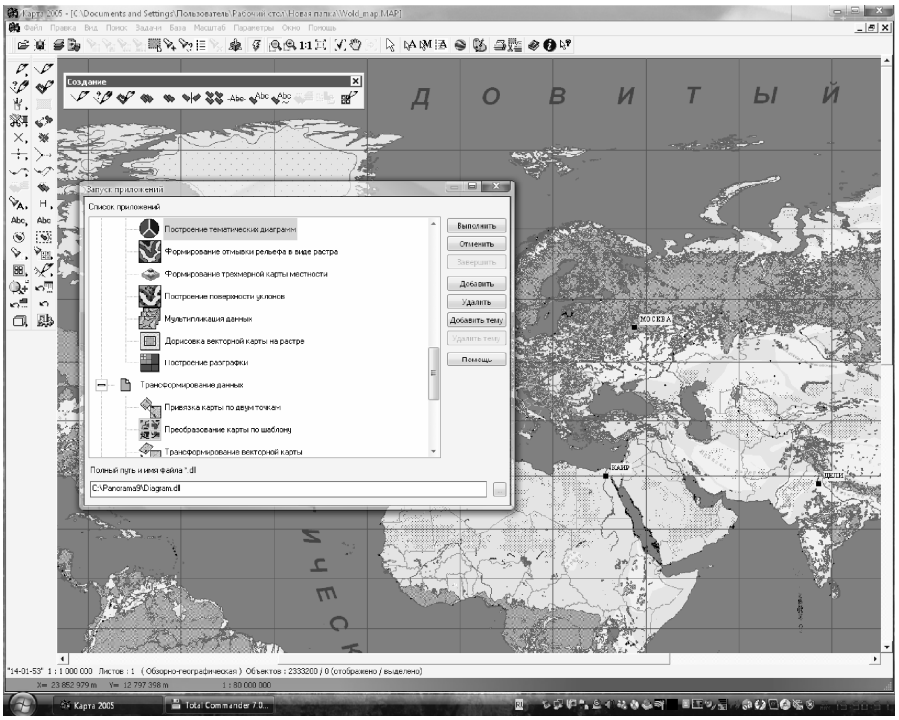


Рис. 3.21. Запуск приложения для организации тематического картографирования

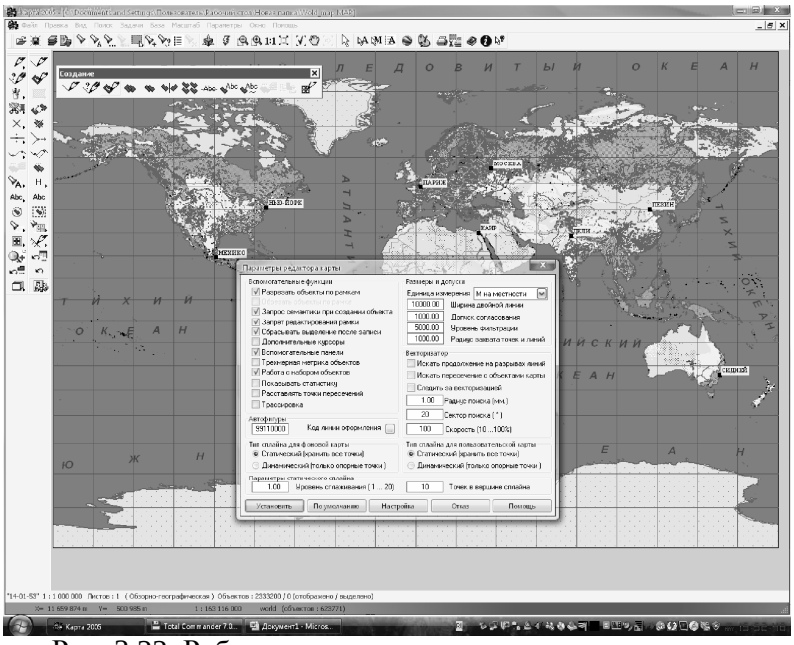


Рис. 3.22. Работа в редакторе карты для организации атрибутивных ссылок

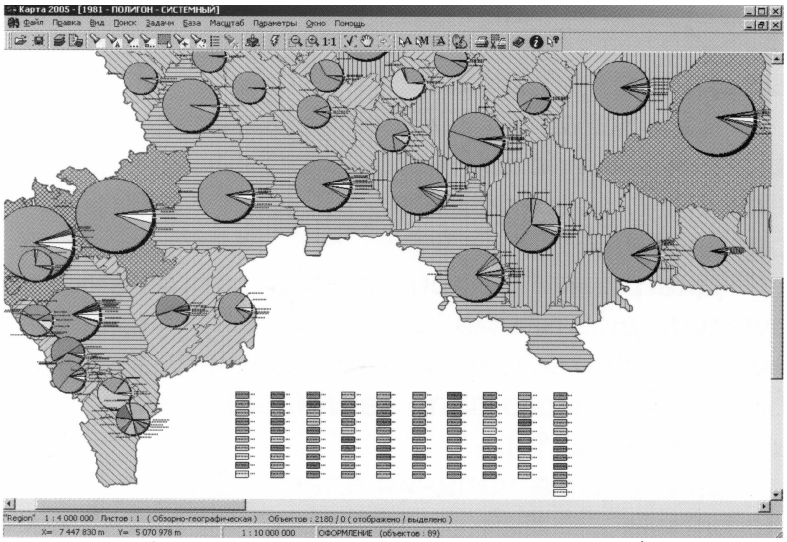


Рис. 3.23. Организация тематического картографирования с привлечением картодиаграмм

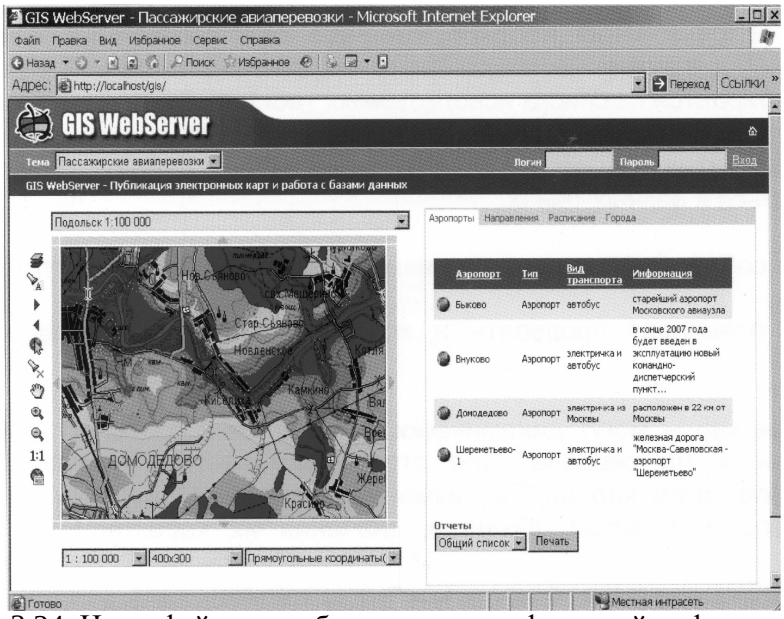


Рис. 3.24. Интерфейс для работы с картографической информацией в виде Web-страниц. Иллюстрация реализации клиент серверной технологии в ГИС «Карта 2005»

3.7.1.4. Особенности серверного доступа к картографической информации в Комплексе визуального анализа «ПФС-ГЕОАНАЛИЗ»

Комплекс визуального анализа (Фирма «ЭРМА-СОФТ») разработан для решения оперативно-аналитических задач с использованием ГИС.

«ПФС-Геоанализ» имеет следующие функциональные характеристики:

- визуализацию, ввод и редактирование картографической и алфавитно-цифровой информации с возможностью динамического пересчета координат при отображении картографической основы;
- отображение космических снимков совместно с картографической основой;
- геокодирование - автоматическое размещение на картографической основе объектов или событий на основе анализа информации с координатами;
- информационно-справочный режим для получения информа-

ции по объектам и событиям, связанным с картографической основой с возможностью сохранения состояния фрагментов карты для быстрого перехода от одного состояния к другому и выполнения поисковых операций для активных слоев и решение некоторых других задач.

«ПФС-ГЕОАНАЛИЗ» позволяет реализовать мультимасштабную картографическую основу, прикрепление атрибутивных данных и вывод различной дополнительной информации (рис. 3.25.), автоматическое размещение атрибутивных данных на карте (рис. 3.26.), связывание данных с местоположений объектов и событий на карте (рис. 3.27.). В ГИС проведена организация серверного доступа к картографической информации (рис. 3.28.).

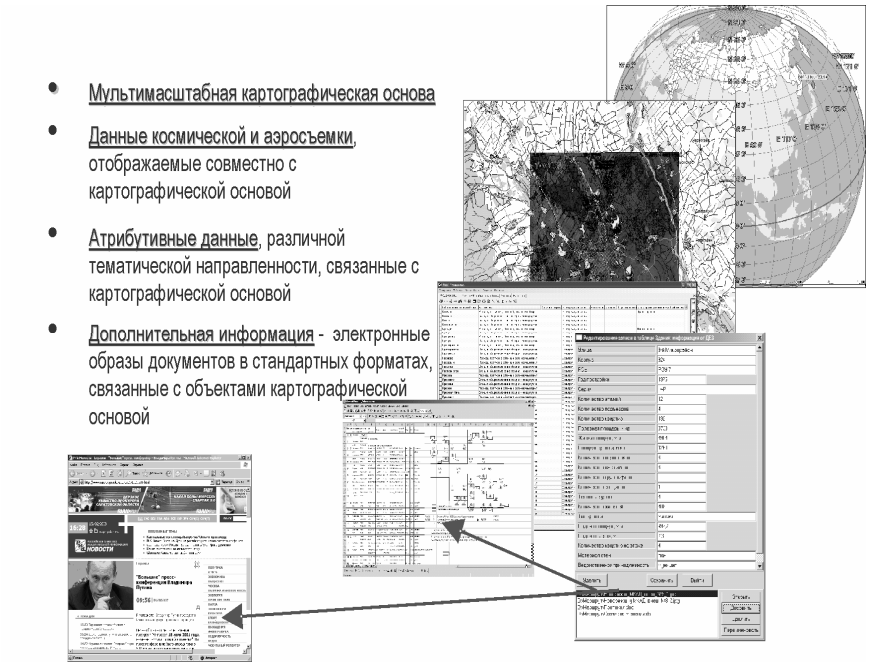


Рис. 3.25. Возможности ПФС «Геоанализ» по прикреплению атрибутивных данных и выводу различной дополнительной информации

Рис. 3.26. Автоматическое размещение атрибутивных данных на карте

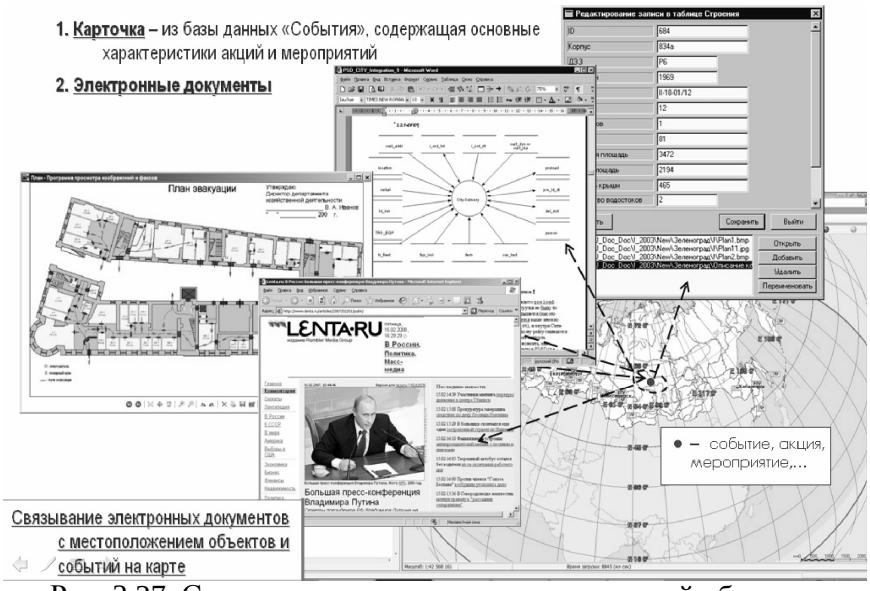


Рис. 3.27. Связывание данных с местоположений объектов и событий на карте

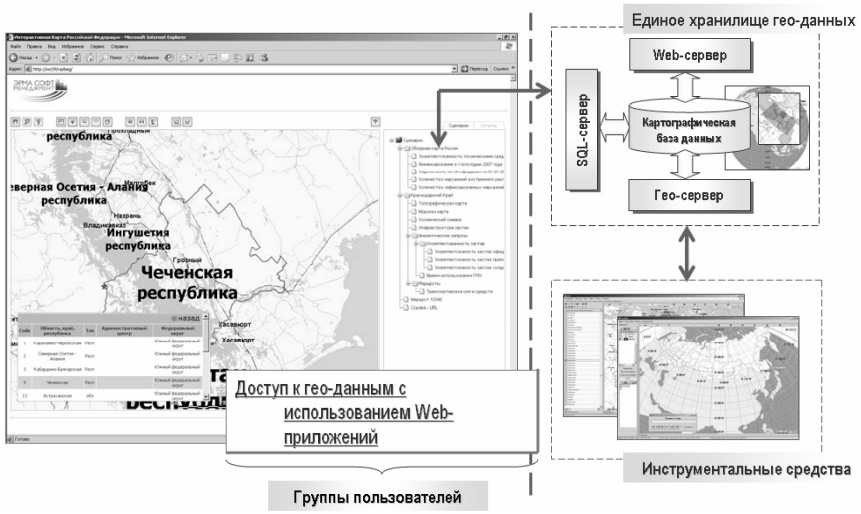


Рис. 3.28. Схема организации серверного доступа к картографической информации

Таким образом, основные преимущества системы «ПФС-Гео-анализ» по сравнению с аналогами заключаются в использовании мультимасштабной картографической основы; возможности подключения данных космической и аэросъемки, отображаемых совместно с картографической основой; использовании атрибутивных данных различной тематической направленности; использовании электронных образов документов в стандартных форматах, связанных с объектами картографической основой.

3.7.1.5. Специальная ГИС для морских пространств - морская информационная система «CARIS LOTS Article 76»

Подкласс ГИС - это специальные ГИС для морских и океанографических пространств, так называемые морские информсистемы. **Их основные задачи - сопровождение вопросов международного морского права; определение границ территориальных вод как основы юридической защиты интересов государства в океане, а также на его дне.**

Среди морских информсистем лидирующие позиции занимает «CARIS LOTS Article 76» (фирма «Universal Systems, Ltd.»). Это специальная ГИС, разработанная для решения проблем определения морских границ. Отличительная черта - ввод данных для сис-

темы из других ГИС и общедоступных наборов данных, например, батиметрических карт и др.

Картографическая база данных ГИС «CARIS LOTS Article 76» была разработана в соответствии с Конвенцией ООН по морскому праву 1982 г. с учетом части IV «Континентальный шельф» Статья 76 «Определение континентального шельфа». В связи с этим данная **ГИС позволяет оперативно вырабатывать позицию государств на переговорах по разграничению морских пространств с сопредельными странами (проведение проверки точности «разменных» площадей и т.п.), своевременно реагировать на кризисные ситуации, которые могут возникнуть с судами вне пределов границ страны.**

Примеры настройки рабочей области и варианты отображаемой информации представлены на рисунках 3.29. - 3.31.

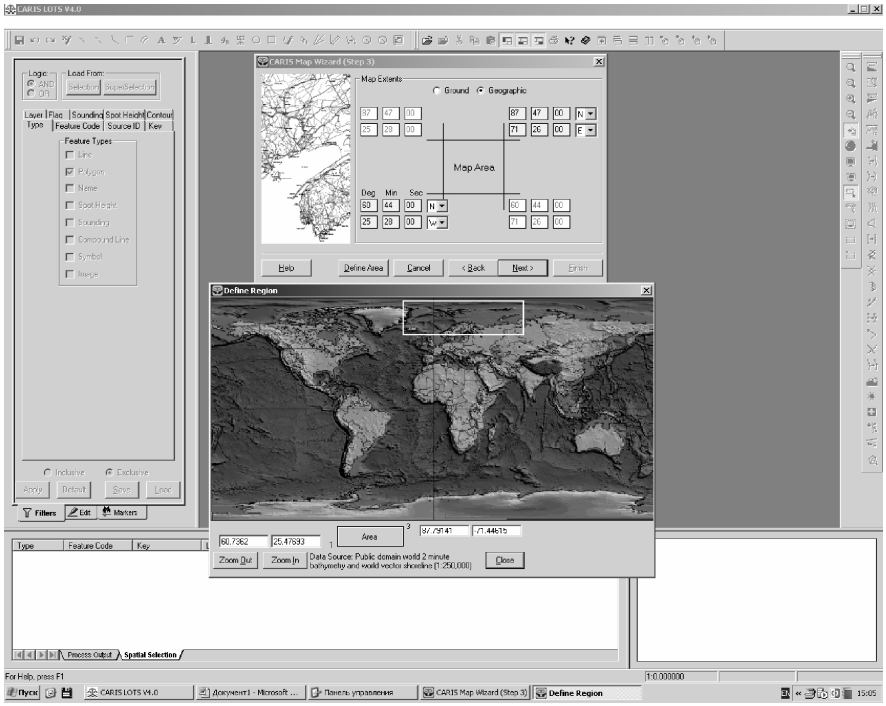


Рис. 3.29. Выбор области карты для проведения анализа

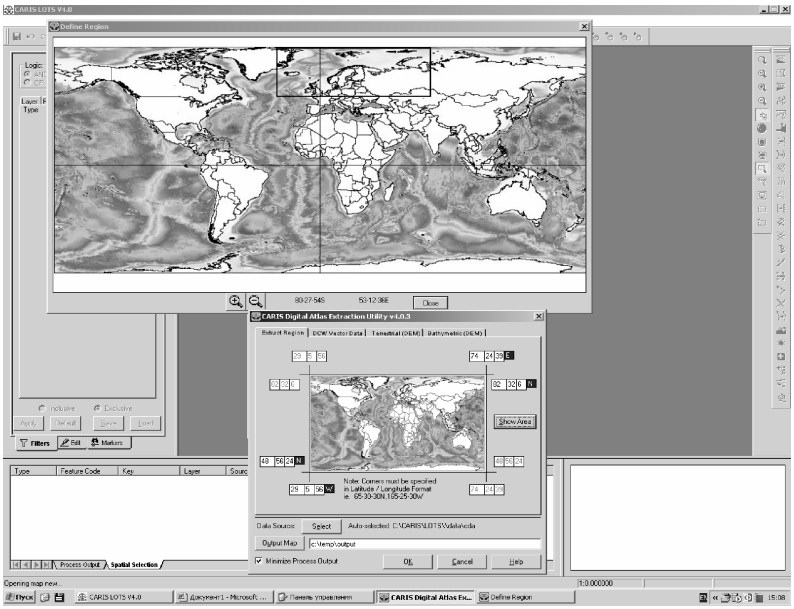


Рис. 3.30. Настройка координатной сетки исследуемой области

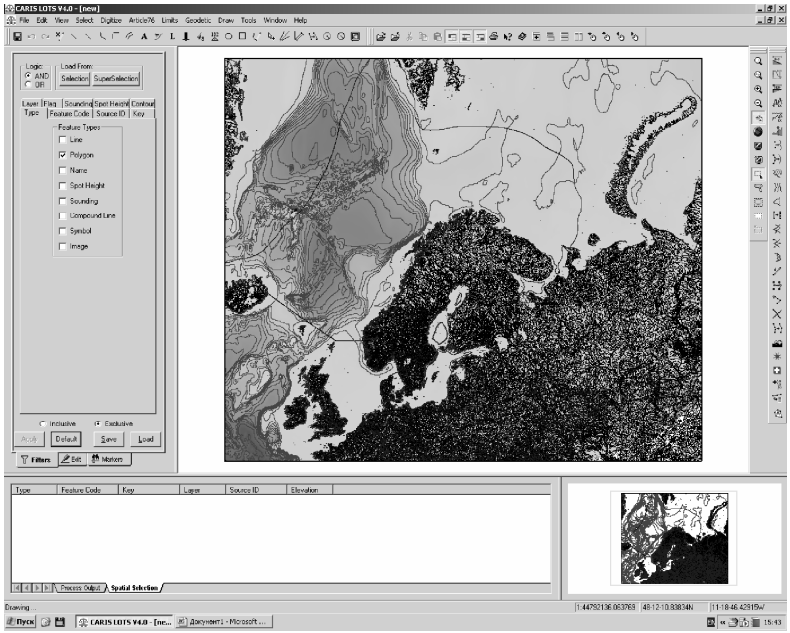


Рис. 3.31. Вид рабочего окна исследуемой области

Таким образом, возможна потребность в данной ГИС со стороны государств, имеющих территориальные воды; компаний, осуществляющих разработку и добычу морских ресурсов; юридических организаций, занимающихся проблемами границ и территориальных споров; а также организаций, работающих в области природопользования.

К недостаткам данной ГИС можно отнести высокую цену, сложность эксплуатации и настройки, связанную, прежде всего, со спецификой решаемых задач, а также необходимость наличия специальных знаний и навыков у операторов данной системы.

3.8. Системы пространственного позиционирования

3.8.1. Глобальные и региональные спутниковые системы навигации

3.8.1.1. Американская система GPS-NAVSTAR

Системы глобального спутникового позиционирования GPS (Global Positioning System) разработаны в США. Аналогичная российская система носит название ГЛОНАСС (Глобальная Навигационная Спутниковая Система).

Система GPS позволяет определять координаты в любой точке земного шара, в любое время, независимо от погодных условий. Точность определения координат колеблется (в зависимости от типов и классов аппаратуры, а также от методики измерений) от 100 м до 1 мм.

Сегодня действует уже второе поколение спутниковых систем позиционирования (ССП). К первому поколению можно отнести системы, разрабатывавшиеся до 70-х гг., главными из которых были NNSS (США) и ЦИКАДА (СССР). NNSS (Navy Navigation Satellite System) - система ВМФ США, позже получившая название TRANSIT. Работы по ее созданию были начаты в 1958 г., в эксплуатации находилась с 1964 г., а с 1967 г. открыта для гражданского применения. К 1980 г. ее услугами пользовались многие тысячи потребителей разных государств. С ее помощью в 1984-1993 гг. в России проводились работы по созданию геодезической сети. Разработки системы ЦИКАДА начаты в 1967 г., в эксплуатацию введена в 1979 г. К первому поколению принадлежит также международная система обнаружения терпящих бедствие COSPAS-SARSAT.

Разработка GPS (параллельное название NAVSTAR - Navigation Satellite Timing and Ranging) и ГЛОНАСС были начаты в 70-х гг. прошлого века. Начало запуска спутников GPS первого блока состоялось в 1978 г., в 1983 г. система открыта для гражданского использования. В 1991 г. сняты ограничения на продажу приемной аппаратуры в Россию.

3.8.1.2. Общие сведения о ГЛОНАСС

Система (ГЛОНАСС) - советская и российская спутниковая система навигации, разработана по заказу Министерства обороны СССР. Одна из двух функционирующих на сегодня систем глобальной спутниковой навигации. Основой системы являются 24 спутника, движущихся над поверхностью Земли в трех орбитальных плоскостях с наклоном орбитальных плоскостей 64,8° и высотой 19 100 км. Принцип измерения аналогичен американской системе навигации GPS- NAVSTAR. В настоящее время развитием проекта ГЛОНАСС занимается Федеральное космическое агентство (Роскосмос) и ОАО «Российские космические системы».

Состав группировки ГЛОНАСС по состоянию на 12.11.2010 г.:

Всего в составе ГЛОНАСС	26 КА
Используются по целевому назначению	20 КА
На этапе ввода в систему	-
Временно выведены на техобслуживание	4 КА
Орбитальный резерв	2 КА
На этапе вывода из системы	-

История развития системы

Первый спутник ГЛОНАСС был выведен в СССР на орбиту 12 октября 1982 г. В 1993 г. система была официально принята в эксплуатацию с орбитальной группировкой из 12 спутников. В 1995 г. спутниковая группировка была развернута до штатного состава - 24 спутника.

Вследствие недостаточного финансирования, а также из-за малого срока службы, число работающих спутников сократилось к 2001 г. до 6.

В 2001 г. была принята ФЦП «Глобальная навигационная система», согласно которой полное покрытие территории России планировалось уже в начале 2008 г. Однако в марте 2008 г. совет глав-

ных конструкторов скорректировал сроки развертывания космического сегмента ГЛОНАСС.

С переходом на спутники «Глонасс-К» точность системы ГЛОНАСС станет сопоставимой с точностью GPS-NAVSTAR - (общее число запущенных спутников NAVSTAR - 60).

В январе 2009 г. было объявлено, что первым городом, где общественный транспорт будет оснащен системой спутникового мониторинга на базе ГЛОНАСС, станет Сочи. На тот момент ГЛОНАСС-оборудование производства компании «M2M телематика» было установлено на 250 сочинских автобусах.

В ноябре 2009 г. было объявлено, что НИИ радиотехнических измерений (г.Харьков) и НИИ космического приборостроения (г.Москва) создадут совместное предприятие и систему спутниковой навигации для потребителей двух стран. В проекте будут использованы украинские станции коррекции для уточнения координат систем ГЛОНАСС.

Технические средства навигации

Рис. 3.32. Экран прибора-навигатора Glospace с отображением плана московских улиц в перспективной проекции и указанием местоположения наблюдателя

Впервые потребительские спутниковые навигаторы, рассчитанные на совместное использование ГЛОНАСС и GPS, поступили в продажу в 2007 г. - это были спутниковые навигаторы Glospace.

Комбинированная ГЛОНАСС/GPS аппаратура профессионального уровня изготавливается многими производителями, в том числе зарубежными фирмами Topcon, Javad, Trimble, Septentrio, Ashtech, NovAtel, SkyWave Mobile Communications.

В целях реализации Постановления Правительства РФ от 25 августа 2008 г. № 641 «Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS» НПО ПРОГРЕСС разработало и выпустило аппаратуру спутниковой навигации ГАЛС-М1 и ГЛИССАДА-А1, которой оснащены многие виды военной и специальной техники.

В настоящее время точность определения координат системой ГЛОНАСС несколько отстает от аналогичных показателей GPS.

На 29 марта 2010 г. ошибки навигационных определений ГЛОНАСС (при p=0,95) по долготе и широте составляли 4,46-8,38 м при использовании в среднем 7-8 КА (в зависимости от точки приема). В то же время ошибки GPS составляли 2,00-8,76 м при использовании в среднем 6-11 КА (в зависимости от точки приема). При совместном использовании обеих навигационных систем ошибки составляют 2,37-4,65 м при использовании в среднем 14-19 КА (в зависимости от точки приема).

Согласно заявлениям главы Роскосмоса А.Перминова, принимаются меры по увеличению точности. К марту 2011 г. с доведением спутниковой группировки до 24 точность системы ГЛОНАСС должна быть улучшена до 2,8 метров. Среди других мер обычно называются увеличение точности эфемерид, улучшение потребительских устройств и постепенная замена спутников на более совершенные Глонасс-М и Глонасс-К.

При этом использование обеих навигационных систем уже сейчас дает существенный прирост точности. Европейский проект EGNOS, использующий сигналы обеих систем, дает точность определения координат на территории Европы на уровне 1-3 метров.

Доступность навигации

Информационно-аналитический центр ГЛОНАСС публикует на своем сайте[74] официальные сведения о доступности навигационных услуг в виде карт мгновенной и интегральной доступности, а также позволяет вычислить зоны видимости для данного места и даты. Оперативный и апостериорный мониторинг систем GPS и ГЛО-

[74] http://www.glonass-ianc.rsa.ru/pls/htmldb/f?p=201:1:3570774877809898

НАСС осуществляет Российская система дифференциальной коррекции и мониторинга (СДКМ).

На 29 марта 2010 г. количество видимых над горизонтом над Россией спутников ГЛОНАСС было равно 7-8 КА. Согласно карте интегральной доступности точность определения координат «хорошая» и лучше (PDOP $\leq$ 6) осуществляется для России практически в течение всего дня (точнее, для 99% времени в течение дня для всей страны кроме района Владивостока, где он равен 95%). В некоторых районах планеты «хорошая» и лучше точность определения координат (PDOP $\leq$ 6) осуществляется в течение 92% времени суток, а в некоторых - в течение 80%.

При совместном использовании ГЛОНАСС и GPS (практически все ГЛОНАСС приемники являются совместными) точность определения координат практически всегда «отличная» вследствие большого количества видимых КА и их хорошего взаимного расположения.

Устройства с поддержкой ГЛОНАСС уже производятся и продаются в США, Канаде, Бельгии, Японии и других странах. Российская навигационная система активно используется в этих странах в геодезии, строительстве, сельском хозяйстве и других отраслях.

3.8.1.3. ГАЛИЛЕО

Галилео (Galileo) - совместный проект спутниковой системы навигации Европейского союза и Европейского космического агентства (ЕКА), является частью транспортного проекта Трансъевропейские сети (англ. Trans-European Networks). **Система Галилео предназначена для решения навигационных задач для любых подвижных объектов с точностью менее одного метра**. Ныне существующие GPS-приемники не смогут принимать и обрабатывать сигналы со спутников Галилео, хотя достигнута договоренность о совместимости и взаимодополнению с системой GPS-NAVSTAR третьего поколения. Финансирование проекта будет осуществляться, в том числе за счет продажи лицензий производителям приемников.

Помимо стран Евросоюза достигнуты договоренности на участие в проекте с такими странами, как Китай, Израиль, Южная Корея, Украина и Россия. Кроме того, ведутся переговоры с представителями Аргентины, Австралии, Бразилии, Чили, Индии, Малайзии. Ожидается, что Галилео войдет в строй в 2014-2016 гг., когда на орбиту будут выведены все 30 запланированных спутников (27 операционных и 3 резервных). Компания Arianespace заключила

договор на 10 ракет-носителей «Союз» для запуска спутников, начиная с 2010 г. Космический сегмент будет дополнен наземной инфраструктурой, включающей в себя три центра управления и глобальную сеть передающих и принимающих станций.

В отличие от американской GPS и российской ГЛОНАСС система Галилео не контролируется национальными военными ведомствами, однако в 2008 г. парламент ЕС принял резолюцию «Значение космоса для безопасности Европы», согласно которой допускается использование спутниковых сигналов для военных операций, проводимых в рамках европейской политики безопасности. Разработку осуществляет ЕКА. Общие затраты на создание системы оцениваются в 4,9 млрд.евро.

Первая фаза - планирование и определения задач, стоимостью в 100 млн.евро, второй этап состоит в запуске двух опытных спутников и развития инфраструктуры (наземных станций для них), его стоимость 1,5 млрд.евро.

Оба спутника GIOVE предназначены для проведения испытаний аппаратуры и исследования характеристик сигналов. Для систематического сбора данных измерений усилиями ЕКА была создана всемирная сеть наземных станций слежения оборудованных приемниками, разработанными в компании Septentrio.

Третий этап состоит в выводе на орбиты четырех спутников Galileo IOV (in-orbit validation), которые, будучи запущенными парами в августе и октябре 2011 г., создадут первое мини-созвездие Galileo. Запуск состоится с помощью ракеты «Союз-СТА» с космодрома в Куру. Первые четыре спутника строятся партнерством EADS Astrium-Thales Alenia Space. Спутники будут расположены на круговых орбитах на высоте порядка 23 тыс.км.

Создание наземного сегмента: трех центров управления (GCC), пяти станций контроля за спутниковой группировкой (TTC), 30 контрольных приемных станций (GSS), 9 ап-линк станций (ULS) для актуализации излучаемых сигналов.

Вывод на орбиту спутниковой группировки

Компания Thales Alenia Space (Италия) обеспечит системную подготовку Galileo, компания OHB-System AG (Германия) произведет (совместно с британской SSTL) спутники первой очереди системы. Первый спутник должен быть готов к июлю 2012 г., впоследствии каждые три месяца должны поставляться очередные два аппарата, объем заказа составляет 566 млн.евро.

Первые виды услуг должны быть представлены в 2014 г., все виды служб - не раньше 2016 г. Общая стоимость проекта на данном этапе - 3,4 млрд.евро.

Четвертый этап проекта будет запущен предположительно с 2014 г., стоимость - 220 млн.евро в год. Возможно, лицензия на эксплуатацию будет передана частным компаниям.

Благодаря найденному компромиссу с правительством США будет применяться формат данных BOC1.1, что позволит взаимодополнять системы GPS и Галилео.

Поисково-спасательная служба

Система для обеспечения приема сигналов бедствия и позиционирования места бедствия с возможностью получения на месте бедствия ответа от спасательного центра. Система должна дополнить, а затем и заменить ныне существующую КОСПАС/САРСАТ. Преимуществом системы над последней является более уверенный прием сигнала бедствия вследствие большей близости к земле и геостационарного положения спутников. Система разработана в соответствии с директивами Международной морской организации (IMO) и должна быть включена в Глобальную морскую систему связи при бедствиях и для обеспечения безопасности мореплавания (ГМССБ).

3.8.1.4. Индийская спутниковая региональная система навигации

9 мая 2006 г. Правительство Индии одобрило проект развертывания Индийской спутниковой региональной системы навигации (IRNSS) в течение последующих 6-7 лет. Спутниковая группировка IRNSS будет состоять из семи спутников на геосинхронных орбитах. Причем четыре спутника из семи в IRNSS будут размещены на орбите с наклонением в 29^{o} по отношению к экваториальной плоскости. Все семь спутников будут иметь непрерывную радиовидимость с Индийскими управляющими станциями.

Земной сегмент IRNSS будет иметь станцию мониторинга, станцию резервирования, станцию контроля и управления бортовыми системами. Государственная компания ISRO является ответственной за развертывание IRNSS, которая будет находиться целиком под контролем Индийского правительства.

3.8.1.5. Китайская навигационная спутниковая система Beidou/Compass

Китай также начал строительство собственной спутниковой системы навигации Compass. Космический сегмент спутниковой системы навигации Beidou/Compass будет сформирован из 5 спутников на Геостационарной орбите (ГСО) и 30 спутников на средней земной орбите.

Планируется предусмотреть два типа услуг. Для общего пользования будет передаваться сигнал, обработка которого позволит добиться точности местоопределения в 10 м, скорости в 0,2 м/с и определения текущего времени с точностью 50 нс. Ограниченный круг пользователей получит возможность измерений с большей точностью.

В 2000 г. были выведены три спутника на ГСО. В 2007 г. Китаем был произведен запуск двух новых спутников системы Beidou/Compass. На декабрь 2010 г. общее число китайских навигационных космических аппаратов на орбите достигло шести. К 2011-2012 гг. Китай должен запустить 12 спутников для завершения первой фазы развертывания системы Compass с охватом Китая и его территорий. Но расширение Compass до глобальной сети займет больше времени, чем планировалось. В итоге система будет состоять из 30 спутников. В итоге система будет состоять из 30 спутников. Военные представители заявили, что система Compass (военное название Tang) будет состоять из 35 спутников[75].

Китай осуществляет сотрудничество с другими странами в разработке спутниковой навигации с целью обеспечения взаимодействия Beidou/Compass с другими глобальными навигационными системами.

3.8.1.6. Японская Quasi-Zenith навигационная система (QZSS)

Первоначально Японская QZSS была задумана в 2002 г. как коммерческая система с набором услуг для подвижной связи, вещания и широкого использования для навигации в Японии и соседних районах Юго-Восточной Азии. Первый запуск спутника для QZSS был запланирован на 2008 г. В марте 2006 г. Японское правительство объявило, что первый спутник не будет предназначен для коммерческого использования и будет запущен целиком на бюджетные

[75] http://gps-club.ru/gps_news/detail.php?ID=59182

средства для отработки принятых решений в интересах обеспечения решения навигационных задач. Только после удачного завершения испытаний первого спутника начнется второй этап, и следующие спутники будут в полной мере обеспечивать запланированный ранее объем услуг. Спутник был успешно запущен в декабре 2010 г.[76]

Всего в спутниковый сегмент войдут 3 спутника, орбиты которых будут выбраны таким образом, чтобы их подспутниковые точки описывали на земной поверхности одну и ту же траекторию с одинаковыми временными интервалами. При этом по крайней мере один спутник будет виден под углом места более 70 градусов в любое время на территории Японии и Кореи. Эта особенность и определила название навигационной системы - Quasi-Zenith. Антенны спутников будут передавать сигналы практически во всей зоне видимости спутников, обеспечивая навигацию и передачу сигналов точного времени. Однако сигналы, которые включают в себя различные поправки, позволяющие повысить точность измерений с помощью сигналов GPS и, возможно, GALILEO, будут передаваться с помощью параболической антенны только на Японию.

Японская QZSS в основном предназначена для улучшения характеристик GPS на национальной и некоторых соседних территориях. Ожидается, что внедрение QZSS позволит существенно повысить эффективность решения навигационных и других задач и придаст ускорение внедрению новых применений для навигации, которые требуют большей точности и надежности.

3.8.1.7. Перспективы спутниковых навигационных систем

В 2007 г. произошла смена лексики: если раньше в основном использовалась аббревиатура **GPS**, подразумевавшая спутниковую навигационную систему, то новой общепринятой аббревиатурой стала **GNSS - Global Navigation Satellite System.** Основная причина такой замены - расширение орбитальной группировки российской ГЛОНАСС, однако на словах GNSS обычно включает и европейскую GALILEO, орбитальная группировка которой два года была представлена единственным экспериментальным спутником. Китайская система обычно при этом не упоминается.

В ближайшей перспективе будут одновременно работать три глобальных навигационных спутниковых системы GPS, ГЛОНАСС (GLONASS) и GALILEO. Практически во всех странах в настоящее время широко используется только GPS, нормальное функциониро-

[76] http://gps-club.ru/gps_news/detail.php?ID=56634

вание которой целиком зависит от правительства США. В некоторых областях, как например диспетчеризация полетов самолетов, использование GPS является неотъемлемой важнейшей составной частью инфраструктуры.

В то же время навигационные системы в ближайшем будущем составят неотъемлемую часть инфраструктуры государства и напрямую будут влиять на глобальную безопасность.

Ни одно государство не может и не хочет в своем развитии зависеть в какой либо области от другого, хотя и дружественного в данный момент, государства. Поэтому поиск альтернативы GPS и привел к созданию GALILEO и присоединению к ней многих развитых государств. Преимущества, которые появляются от присоединения к альтернативной навигационной системе на этапе ее развития следующие:

- диверсификация рисков, связанных с работой GNSS, посредством диверсификации инфраструктуры земного сегмента и используемого оборудования;
- создание новых рабочих мест при условии разработки и экспорта нового оборудования для GNSS;
- возможность заблаговременного внедрения технологических преимуществ использования GNSS в системы связи, транспорта и развитие новых технологий.

3.8.2. Вопросы международного обмена геопространственной информацией

Геопространственная информация (ГПИ) - совокупность данных о местности и объектах, расположенных на поверхности Земли (планеты или другого небесного тела), в подповерхностном слое Земли, приповерхностном слое атмосферы Земли и околоземном пространстве, необходимых для использования в различных областях деятельности человечества (согласно постановлению Правительства России от 28 мая 2007 г. № 326 «О порядке получения, использования и предоставления геопространственной информации»).

Глобальная система наблюдения Земли (ГСНЗ). (GEOSS: The Global Earth Observation System of Systems http://www.earthobservations.org). Всемирная конференция по устойчивому развитию, состоявшаяся в г.Йоханнесбурге (ЮАР) в 2002 г., выдвинула на первый план необходимость координации усилий по наблюдению состояния Земли, которая подтверждалась.

на саммитах «Группы восьми» и других международных организаций.

Назначение ГСНЗ заключается в обеспечении согласованного, всестороннего и непрерывного наблюдения Земли с целью улучшения мониторинга ее состояния, расширения понимания происходящих на Земле процессов и обеспечения более надежного прогноза поведения земных систем. **Информация, собранная в интересах ГСНЗ - двойного назначения**.

На саммите в Брюсселе (2005 г.) были учреждены Группа наблюдения за Землей (ГНЗ, включает 70 стран-членов) и Исполком ГНЗ, в который входят представители 12 стран - Россия, Бразилия, Германия, Гондурас, Еврокомиссия, Италия, КНР, Марокко, США, Таиланд, ЮАР, Япония.

Штаб-квартира - Женева (при офисе Всемирной метеорологической организации), региональные офисы - Бонн, Пекин.

В 2006 г. Правительством России утверждена Концепция нашего участия в ГСНЗ и построения российского сегмента ГСНЗ (Концепция). В феврале 2007 г. создана Межведомственная комиссия по ГСНЗ, которой руководит Росгидромет (второе головное ведомство - Роскосмос).

10-летний План действий ГСНЗ, по сути уставной документ, включающий в себя не только программу действий, но и структуру и управление организацией, процедурные вопросы принятия решений, финансовые вопросы. Был предложен к рассмотрению на Брюссельском саммите в 2005 г., тогда же был одобрен, но не утвержден.

СПАЙДЕР. 14 декабря 2006 г. на Генеральной Ассамблее ООН в Нью-Йорке была принята резолюция 61/110 об учреждении Платформы ООН по использованию космической информации для предупреждения и ликвидации чрезвычайных ситуаций экстренного реагирования (СПАЙДЕР) и осуществлять ее в качестве одной из программ Управления по вопросам космического пространства Комитета ООН по использованию космического пространства в мирных целях во главе с директором этого Управления.

Штаб-квартира Вена, представительства - Бонн, Пекин, Женева.

В состав входит 41 государство-член и 13 межправительственных и неправительственных организаций (число участников растет).

Уставных документов нет (вместо него план работы на 2007-2009 годы).

Россия с 2006 г. участвует в организации, головные ведомства МЧС и Роскосмос.

Для снижения последствий, предупреждения и ликвидации стихийных и других бедствий (цунами в Юго-восточной Азии, наводнений в Европе и Северной Америке, землетрясений в Южной Азии) перед международным сообществом стал актуальным вопрос международного обмена геопространственной информацией (ГПИ).

Кроме того, с развитием новейших ИКТ, ГПИ становится неотъемлемой частью как инновационного развития государств (промышленность, строительство, транспорт, сельское хозяйство, наука, коммуникации и др.), так и каждодневной необходимостью каждого человека (прогноз погоды, отдых, туризм и т.д). Речь идет, прежде всего, об информации, полученной в результате дистанционного зондирования Земли (ДЗЗ) и других небесных тел. Все эти вопросы имеют огромное значение для социально-экономического развития Российской Федерации, затрагивают вопросы национальной безопасности.

В деятельность по получению ГПИ вовлекается все больше и больше стран. Особую активность проявляют США, ЕС, Япония, КНР, Индия, Бразилия, ЮАР. Традиционно в этом семействе достаточно серьезно была представлена Россия.

По инициативе США были созданы Глобальная система наблюдения Земли (ГСНЗ) и **платформа ООН для использования космической информации для предупреждения и ликвидации чрезвычайных ситуаций и экстренного реагирования, создаваемая под эгидой Комитета ООН по использованию космического пространства в мирных целях (СПАЙДЕР).**

Проблематика обмена информацией, и, прежде всего ГПИ, является ключевой в повестке работы ГСНЗ и СПАЙДЕРА.

Глава 4
МЕТОДЫ ПРОГНОЗИРОВАНИЯ НАПРАВЛЕНИЙ РАЗВИТИЯ МЕЖДУНАРОДНЫХ КОНФЛИКТОВ

Если Вы не думаете о будущем,
у Вас его не будет.

Дж.ГОЛСУОРСИ

Рост конфликтного потенциала в мире диктует необходимость не только анализировать конфликты, но и прогнозировать их.

Актуальность поставленной задачи определяется тем, что прогнозирование конфликтов позволяет решить многие проблемы, вызванные столкновением интересов субъектов межгосударственных отношений, на ранних стадиях конфликта политико-дипломатическими средствами, чтобы разрешить их или минимизировать наносимый ущерб.

Под прогнозированием развития международного конфликта (МК) понимается расчет текущего состояния (фазы) МК и определение сценария дальнейшего развития конфликта, т.е. событий, которые могут произойти в прогнозируемый промежуток времени.

4.1. Фазово-факторная модель международного конфликта

Ядром предлагаемой методики прогнозирования является фазово-факторная модель международного конфликта (МК), разработанная на основе известной модели МК, предложенной Л.Блумфилдом и А.Лейс и используемая в системе CASCON[77]. В ней МК представляется, как динамический процесс, проходящий цепь явно идентифицируемых **фаз**. Под фазами понимаются различные состояния конфликта. Таких фаз шесть: мирное сосуществование (фаза введена нами), диспут, конфликт, военные дей-

[77] Кретов В.С., Котов М.Н. Фазово-факторная модель межгосударственного конфликта // II Международная научно-практическая конференция «Инновационное развитие российской экономики»: Сборник научных трудов Московский государственный университет экономики, статистики и информатики – М., 2009, С. 447-448

ствия, прекращение военных действий, урегулирование. В рамках конфликта фазы могут сменять друг друга в любом направлении.

В фазово-факторной модели (рис. 4.1.) каждая фаза обладает параметром - **весом фазы** в конфликте[78], который показывает возможность нахождения данного конфликта в этой фазе в заданный промежуток времени. Чем больше вес фазы при расчетах, тем больше возможность того, что конфликт находится в этой фазе в рассматриваемый промежуток времени.

Каждая фаза определяется множеством **факторов**. Под факторами подразумеваются заложенная в них информация о событиях, явлениях, действиях и т.д., которая указывала бы на то, что конфликт находится в фазе, определяемой этим фактором. Каждый фактор наделен параметром - **степенью влияния** фактора на соответствующую ему фазу. Он показывает, как сильно повлияет свершение события, заложенного в данный фактор, на вес соответствующей фазы.

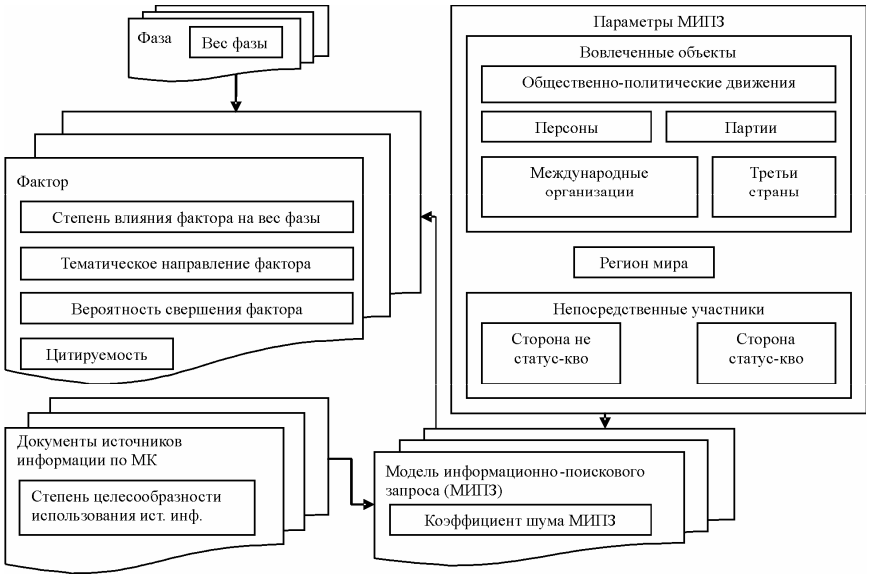


Рис. 4.1. Фазово-факторная модель международного конфликта

[78] Кретов В.С., Котов М.Н. Методика выбора источников информации при анализе фазы международного конфликта // Ситуационные центры и перспективные информационно-аналитические средства поддержки принятия решений. Материалы научно-практической конференции, состоявшейся в РАГС 7-9 апреля 2008 г. / Под общ. ред. А.Н.Данчула. - М.: Изд-во РАГС, 2009

Все факторы классифицированы независимо от принадлежности к фазе конфликта по **тематическим направлениям** (отношения конфликтующих сторон, военно-политические вопросы, международные организации в конфликте, этнические вопросы, экономика и ресурсы, внутренняя политика конфликтующих сторон, информация и пропаганда, ситуация на спорных территориях). Это позволяет рассматривать конфликт в различных аспектах, а также обобщать специфические свойства конфликта и использовать их для сравнения и классификации.

Важным параметром фактора является **вероятность свершения фактора**, которая позволяет оценить вероятность свершения события, заложенного в фактор.

Каждый фактор определяется **цитируемостью** во времени. Цитируемость - это частота выявления фактора в используемых источниках информации, т.е. это частота с которой появляется информация о свершении событий, заложенных в фактор в СМИ. Свершение фактора происходит в том случае, когда информация о событии или сведения об объекте, соответствующие фактору стали доступными.

Для автоматического определения цитируемости факторов в документах каждому фактору ставится в соответствие его **модель информационно-поискового запроса (МИПЗ)**, обладающая параметрами. В качестве параметров выступают: непосредственные участники конфликта (сторона статус-кво, сторона не статус-кво); вовлеченные объекты (общественно-политические движения, персоны, партии, международные организации, третьи страны); регион мира (территория, на которой протекает межгосударственный конфликт). Описание факторов с помощью МИПЗ осуществляется при помощи специального языка. Этот язык использует логические операции и операции близости слов.

При описании фактора моделью информационно-поискового запроса следует учитывать **коэффициент шума** этой модели. Он позволяет оценить соответствие информации, найденной в различных источниках при помощи этой модели, смыслу фактора. Коэффициент шума модели информационно-поискового запроса уточняет возможность присутствия соответствующего фактора в тексте документа источника информации, что в свою очередь влияет на вес соответствующей фазы.

Для оценки источников информации введем понятие **степень целесообразности**. Под степенью целесообразности подразумевается возможность использования источника информации для анализа МК. Оценку степени целесообразности использования инфор-

мации, предлагаемой источником, для исследования МК следует проводить по тематическим направлениям. Т.к. информация, поступающая из одного и того же источника, может удовлетворять необходимым требованиям, например, по «военно-политическому» направлению, но в тоже время не будет удовлетворять аналогичным требованиям по «экономико-ресурсному» направлению.

В рамках фазово-факторной модели введено понятие **сценария дальнейшего развития МК.** В терминах фазово-факторной модели сценарий дальнейшего развития МК определяется как множество факторов, которые возможно произойдут в течение прогнозируемого периода. Каждый фактор сценария определяется показателем свершения. Под показателем свершения фактора подразумевается возможность свершения события, заложенного в фактор в прогнозируемый промежуток времени.

4.2. Общая схема прогнозирования развития международного конфликта

Общая схема прогнозирования развития международного конфликта (МК) представлена на рис. 4.2.

Сначала при помощи интеллектуальной ИПС «Истра-2006» получаем коэффициенты шума МИПЗ факторов и цитируемость факторов во всех используемых источниках информации. Далее при помощи прикладных научных методов рассчитывается степень влияния факторов на фазу и степень целесообразности использования источников информации. Затем, на основании полученных результатов, рассчитывается вероятность свершения факторов. Далее рассчитывается фаза, определяющая текущее состояние МК, а также факторы сценария дальнейшего развития МК и их показатели.

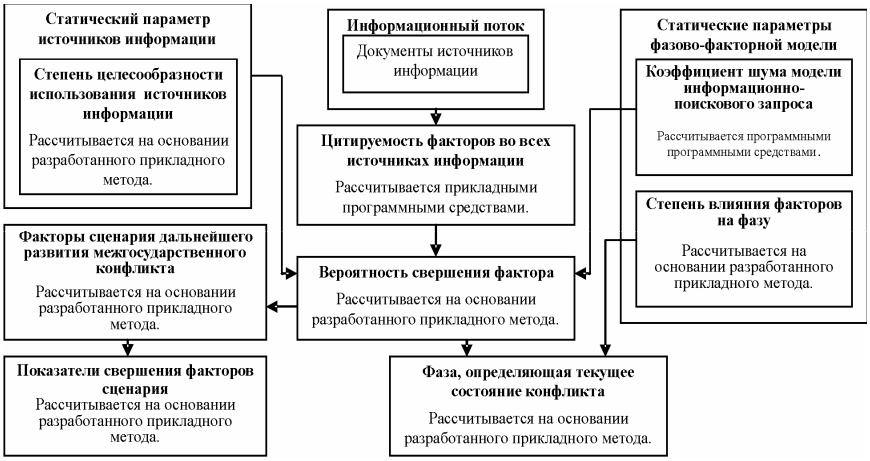


Рис. 4.2. Общая схема прогнозирования развития международного конфликта

При создании методики прогнозирования развития МК было разработано пять прикладных научных методов.

4.2.1. Метод расчета степени влияния факторов на фазу межгосударственного конфликта

Согласно фазово-факторной модели, связь фаз конфликта и факторов представляет собой иерархическую систему, т.е. каждой фазе соответствует набор факторов. Свершение каждого заложенного в фактор события влияет на вес соответствующей фазы в соответствии со степенью влияния фактора на фазу (рис. 4.3.).

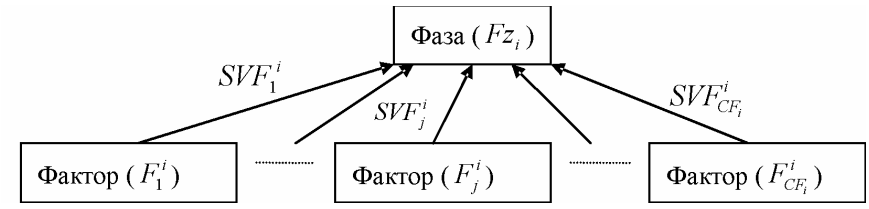


Рис. 4.3. Связь фаз и факторов

где Fz_i - фаза $i, i = 1...CFz, CFz = 6$ - количество фаз, F_j^i - j-й фактор, принадлежащий i - ой фазе, $j = 1...CF^i$, где CF^i - количество факторов описывающих i-ую фазу.

Для расчета степени влияния фактора на фазу используется метод парных сравнений, который позволяет сравнить факторы, относительно их влияния на соответствующую фазу, т.е. получить степени влияния факторов.

Для получения степени влияния факторов на соответствующую им фазу эксперту необходимо заполнить матрицы парных сравнений степеней влияния факторов на соответствующую фаз. Таких матриц 6, что соответствует количеству фаз (Табл.1).

Таблица 1. Матрица парных сравнений степеней влияния факторов фазы i.

	Факторы				
Факторы		F_1^i	F_2^i	.....	$F_{CF^i}^i$
	F_1^i	1	$VF_{1,2}^i$	.....	VF_{1,CF^i}^i
	F_2^i	$1/VF_{1,2}^i$	1	$VF_{2,k}^i$	⋮
			$1/VF_{2,k}^i$	1	⋮
	$F_{CF^i}^i$	$1/VF_{1,CF^i}^i$	.....	.....	1

где Mf^i - обратно-симметричная матрица парных сравнений степеней влияния множества факторов F_j^i на фазу i, VF_{jk}^i - степень влияния i -ого фактора (F_j^i) относительно j -ого фактора (F_k^i) на фазу i.

Эксперты заполняют ячейки матриц, находящиеся выше главной диагонали значениями от 1 до 9. Элементы, находящиеся на главной диагонали матрицы, равны 1. Элементы, находящиеся ниже главной диагонали матрицы, равняются обратным значениям симметричных им элементов, значения которых выставляет эксперт.

Тогда, согласно методу парных сравнений, степень влияния факторов на фазу представляет собой собственный вектор, соответствующий максимальному собственному значению обратно-сим-

метричной матрицы парных сравнений степеней влияния факторов на фазу.

$$Mf^{i} * SVF^{i} = \lambda_{\max} * SVF^{i} \quad (1)$$

где SVF^{i} - вектор степеней влияния факторов на i - ую фазу, $\lambda_{\max}$ - максимальное собственное значение матрицы Mf^{i}.

Показателем согласованности мнения эксперта является индекс согласованности.

$$Is_{i} = \frac{\lambda_{\max} - CF^{i}}{CF^{i} - 1} \quad (2)$$

где Is_{i} - индекс согласованности мнения эксперта для i - ой фазы, CF^{i} - количество факторов описывающих i -ую фазу.

Если он меньше порогового значения, то суждения эксперта - удовлетворительны, в противном случае матрица сравнений должна быть пересмотрена.

4.2.2. Метод расчета степени целесообразности использования источников информации

Степень целесообразности использования источников информации рассчитывается с применением технологии нейронных сетей по каждому тематическому направлению отдельно, поскольку возможность использования источников информации по одному тематическому направлению не гарантирует возможности его использования по-другому. Для анализа источников информации по каждому тематическому направлению сначала необходимо построить нейронную сеть, а затем ее обучать[79]. С учетом специфики задачи, требуемая нейронная сеть имеет следующий вид (рис. 4.4.).

[79] Котов М.Н. Оценка текущей фазы и определение сценария дальнейшего развития межгосударственного конфликта // Ситуационные центры 2009. Перспективные информационно-аналитические технологии поддержки принятия решений. Материалы научно-практической конференции, состоявшейся в РАГС 14-15 апреля 2009 г. / Под общ. ред. А.Н.Данчула. - М.: Изд-во РАГС, 2010

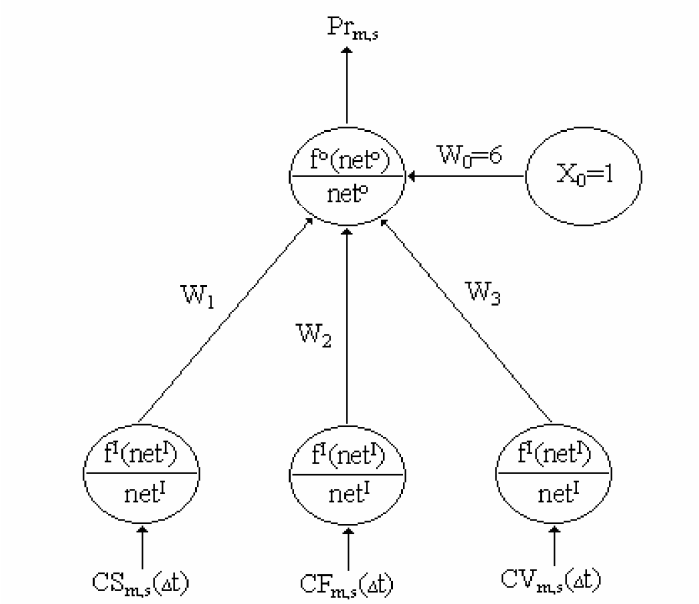


Рис. 4.4. Вид нейронной сети, используемой в методе

где $\mathrm{Pr}_{m,s}$ - степень целесообразности использования m -ого источника информации по s -ому тематическому направлению, $CS_{m,s}(\Delta t)$ - относительная цитируемость s-ого тематического направления в сообщениях m-ого источника информации в интервале времени Δt, $CF_{m,s}(\Delta t)$ - относительная цитируемость факторов соответствующих s-ому тематическому направлению в m-ом источнике информации в интервале времени Δt, $CV_{m,s}(\Delta t)$ - средняя частота цитируемости s-ого тематического направления в m-ом источнике информации в интервале времени Δt, net^I, net^o - правило комбинирования входных сигналов, $f^I(net^I)$, $f^o(net^o)$ - функция активности, определяющая правило вычисления выходного сигнала, который будет передан элементам следующего слоя, W_{s1}, W_{s2}, W_{s3} - весовые коэффициенты.

$$CS_{m,s}(\Delta t) = \frac{CSN_{m,s}(\Delta t)}{CSA_m(\Delta t)} \qquad (3)$$

где $CSN_{m,s}(\Delta t)$ - количество сообщений из m - ого источника информации, в которых представлены факторы соответствующие s - ому тематическому направлению в интервале времени Δt, $CSA_m(\Delta t)$ - общее количество сообщений m - ого источника в интервале времени Δt.,

$$CF_{m,s}(\Delta t) = \frac{CFN_{m,s}(\Delta t)}{CFA_s} \quad (4)$$

где $CFN_{m,s}(\Delta t)$ - количество факторов соответствующих s - ому тематическому направлению присутствующих в информации из m - ого информационного источника в интервале времени Δt, CFA_s - общее количество факторов соответствующих s - ому тематическому направлению.

$$CV_{m,s}(\Delta t) = \frac{CFN_{m,s}(\Delta t)}{CVA_m(\Delta t)} \quad (5)$$

где $CVA_m(\Delta t)$ - общий объем сообщений в килобайтах m - ого источника в интервале времени Δt.

$$f^I(net^I) = net^I \quad (6)$$

$$net^o = W_{s1} * CS_{m,s}(\Delta t) + W_{s2} * CF_{m,s}(\Delta t) + W_{s3} * CV_{m,s}(\Delta t) + W_0 * X_0 \quad (7)$$

$$f^o(net^o) = \frac{1}{\left(1 + e^{-net^o}\right)} \quad (8)$$

На выходе нейронной сети рассчитывается степень целесообразности использования источника информации по отдельно взятому тематическому направлению. Прежде чем использовать нейронную сеть ее необходимо обучить на обучающем множестве источников согласно схеме (рис. 4.5.).

Сначала документы источников информации из обучающего множества фильтруются по тематическим направлениям. Далее документы в каждом тематическом фильтре группируются по источникам. После чего сгруппированные данные подаются на вход нейронной сети. Для обучения нейронной сети используется алгоритм обратного распространения ошибок. В результате обучения получаем величины, в соответствии с которыми следует корректировать весовые коэффициенты W_{s1}, W_{s2}, W_{s3}.

$$\Delta W_{s,k} = \eta_s * \left(\Pr{}^{o}_{m,s} - \Pr_{m,s}\right) * f^{o}\left(net^{o}_{m,s}\right) * \left(1 - f^{o}\left(net^{o}_{m,s}\right)\right) * X_{m,s,k} \quad (9)$$

где $\Pr{}^{o}_{m,s}$ - степень целесообразности использования m - ого источника информации по s - ому тематическому направлению.

Обучение продолжается до тех пор, пока значение выходного сигнала для каждого обучающего источника не окажется в рамках допустимого отклонения (0,01) от соответствующего целевого выходного образца (рис. 4.6.).

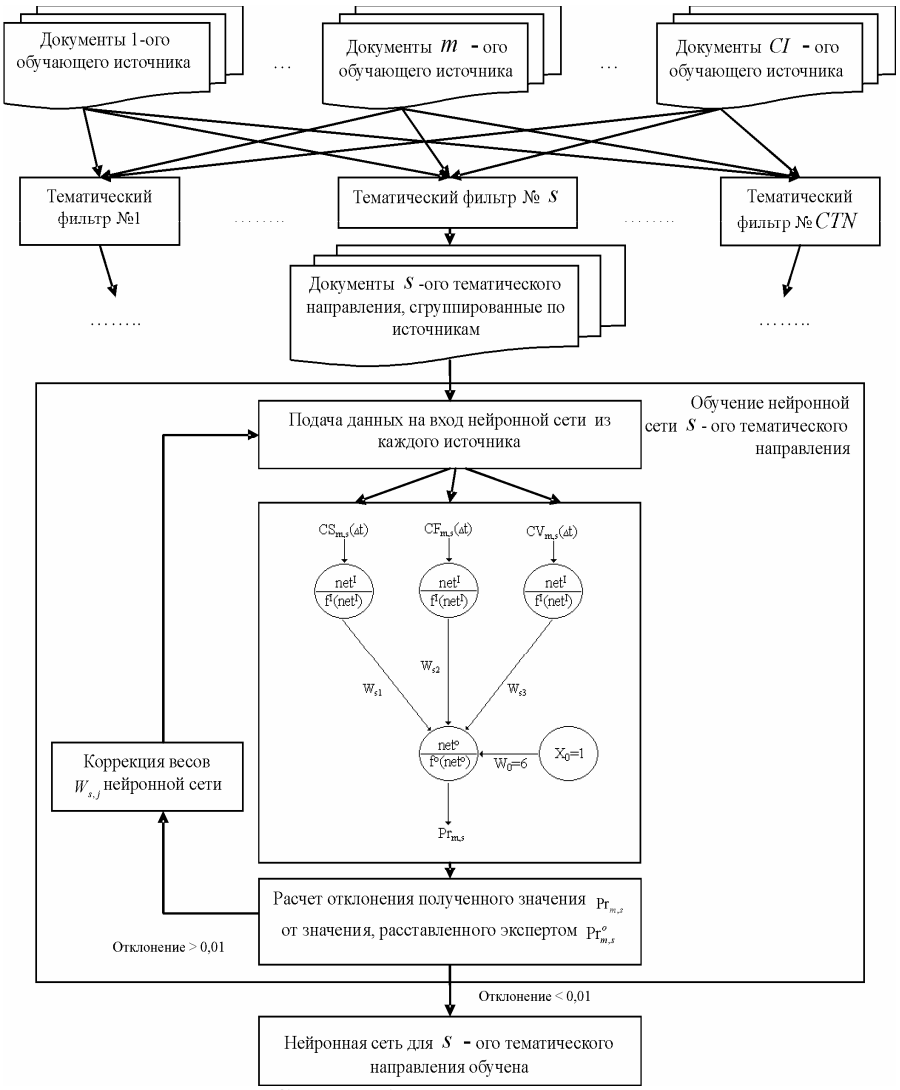


Рис. 4.6. Схема обучения нейронной сети

где CI - количество обучающих источников информации, CTN - количество тематических направлений.

После того, как нейронная сеть построена и обучена, ее можно использовать для вычисления степеней целесообразности использования источников информации по тематическим направлениям.

4.2.3. Метод оценки вероятности свершения фактора

Под *вероятностью* свершения фактора понимается вероятность того, что по информации хотя бы одного источника событие, заложенное в фактор, свершилось. Метод использует следующие исходные данные: коэффициенты шума моделей информационно-поисковых запросов факторов, данные о цитируемости факторов в источниках информации, а также полученные на основании представленного метода данные степеней целесообразности использования источников информации.

Коэффициент шума МИПЗ рассчитывается по формуле:

$$NF_j^i = \frac{NL_j^i}{NO_j^i} \tag{10}$$

где NF_j^i - коэффициент шума МИПЗ фактора j фазы i, NL_j^i - количество выявлений фактора j фазы i, при которых найденная информация соответствует смыслу, заложенному в фактор, NO_j^i - общее количество выявлений фактора j фазы i.

Цитируемость факторов представлена в виде таблиц.

Таблица 2. Таблица значений цитируемости всех факторов по всем источникам.

	Источники			
Факторы i-ой фазы	$QF_{1,1}^i$	…….	…….	$QF_{1,CI}^i$
	⋮	…….	…….	⋮
	⋮	…….	…….	⋮
	$QF_{CF^i,1}^i$	…….	…….	$QF_{CF^i,CI}^i$

где $QF_{j,m}^i$ - значение цитируемости фактора j фазы i в источнике m.

Количество таких таблиц соответствует количеству фаз конфликта.

Согласно методу, сначала рассчитаем вероятность свершения фактора на основании информации, предоставленной одним источником.

$$VSF_{jm}^{i} = 1 - \left(1 - NF_{j}^{i}\right)^{QF_{jm}^{i}} \quad (11)$$

где VSF_{jm}^{i} - вероятность свершения j - ого фактора i - ой фазы по информации из m - ого источника, NF_{j}^{i} - коэффициент шума МИПЗ фактора j фазы i.

Затем учитываем степень целесообразности использования источника информации.

$$VSF_{jm}^{i} = \Pr_{ms} * \left(1 - \left(1 - NF_{j}^{i}\right)^{QF_{jm}^{i}}\right) \quad (12)$$

где $\Pr_{ms}$ - степень целесообразности использования m - ого источника по s - ому тематическому направлению.

И, наконец, на основании полученных результатов рассчитываем вероятность свершения фактора по материалам всех используемых источников.

$$VSF_{j}^{i} = 1 - \left(1 - \Pr_{ms} * \left(1 - \left(1 - NF_{j}^{i}\right)^{QF_{jm}^{i}}\right)\right)^{CI} \quad (13)$$

где CI - количество используемых источников информации.

4.2.4. Метод расчета определяющей фазы международного конфликта

Согласно фазово-факторной модели свершение каждого фактора влияет на вес соответствующей фазы с учетом рассчитанной степени влияния фактора на фазу[80]. Поэтому итоговое влияние фак-

[80] Котов М.Н. Оценка текущей фазы и определение сценария дальнейшего развития межгосударственного конфликта // Ситуационные центры 2009. Перспективные информационно-аналитические технологии поддержки принятия решений. Материалы научно-практической конференции, состоявшейся в РАГС 14-15 апреля 2009 г. / Под общ. ред. А.Н. Данчула. - М.: Изд-во РАГС, 2010

тора на соответствующую ему фазу будет определяться по формуле.

$$IVF_j^i = SVF_j^i * VSF_j^i \quad (14)$$

где IVF_j^i - итоговое влияние фактора j на соответствующую фазу i, SVF_j^i - степень влияния фактора j на фазу i, VSF_j^i - вероятность свершения фактора j фазы i.

Вес фазы рассчитывается как средние значения итоговых степеней влияния факторов, описывающих данную фазу.

$$Fz^i = \frac{\sum_{j=1}^{CF^i} IVF_j^i}{CF^i} \quad (15)$$

где Fz^i - вес i - ой фазы, CF^i - количество факторов описывающих i - ую фазу.

Теперь рассчитаем определяющую фазу конфликта. Для этого необходимо построить и обучить нейронную сеть.

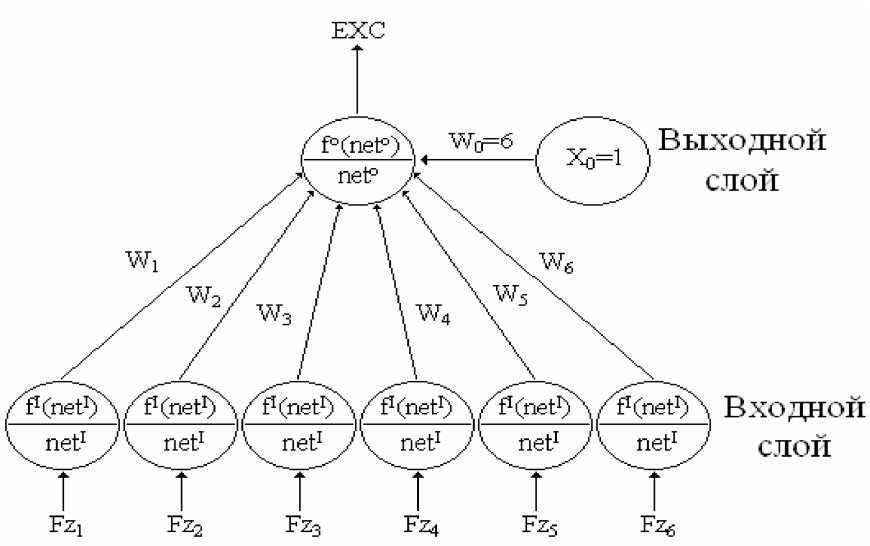


Рис. 4.7. Вид нейронной сети, используемой в алгоритме

где EXC - единая характеристика конфликта, принимает значения от 0 до 1 и показывает состояние конфликта в рассматриваемый момент времени, Fz^i - вес i - ой фазы, net^I, net^o - правило комбинирования входных сигналов, $f^I\left(net^I\right)$, $f^o\left(net^o\right)$ - функция активности, определяющая правило вычисления выходного сигнала, который будет передан элементам следующего слоя, $W_{s,i}$ - весовые коэффициенты.

$$f^I\left(net^I\right) = net^I \tag{16}$$

$$net^o = W_1 * Fz_1 + \ldots + W_{CFz} * Fz_{CFz} + W_0 * X_0 \tag{17}$$

$$f^o\left(net^o\right) = \frac{1}{1+e^{-net^o}} \tag{18}$$

Для обучения нейронной сети используется алгоритм обратного распространения ошибок, описанный ранее (рис. 4.7.).

$$\Delta W_{s,k} = \eta_s * \left(\mathrm{Pr}^o_{m,s} - \mathrm{Pr}_{m,s}\right) * f^o\left(net^o_{m,s}\right) * \left(1 - f^o\left(net^o_{m,s}\right)\right) * X_{m,s,k} \tag{19}$$

Далее по полученной единой характеристике EXC определим фазу, в которой находится межгосударственный конфликт с использованием классификации относительно центров классов.

Для расчета определяющей фазы исследуемого конфликта введем классы, соответствующие фазам «Мирное сосуществование», «Диспут», «Конфликт», «Военные действия», «Прекращение военных действий», «Урегулировании» и зададим область определения в виде $X = [0;1]$. В роли базовой шкалы будет использоваться единая характеристика конфликта EXC .

В качестве функции принадлежности для каждого класса возьмем гауссову функцию.

$$Mc(x) = e^{-\left(\frac{x-c}{\sigma}\right)^2} \tag{20}$$

где c - середина диапазона, σ - кривизна функции.

На рисунке 4.8. изображена совокупность кривых принадлежности для всех классов.

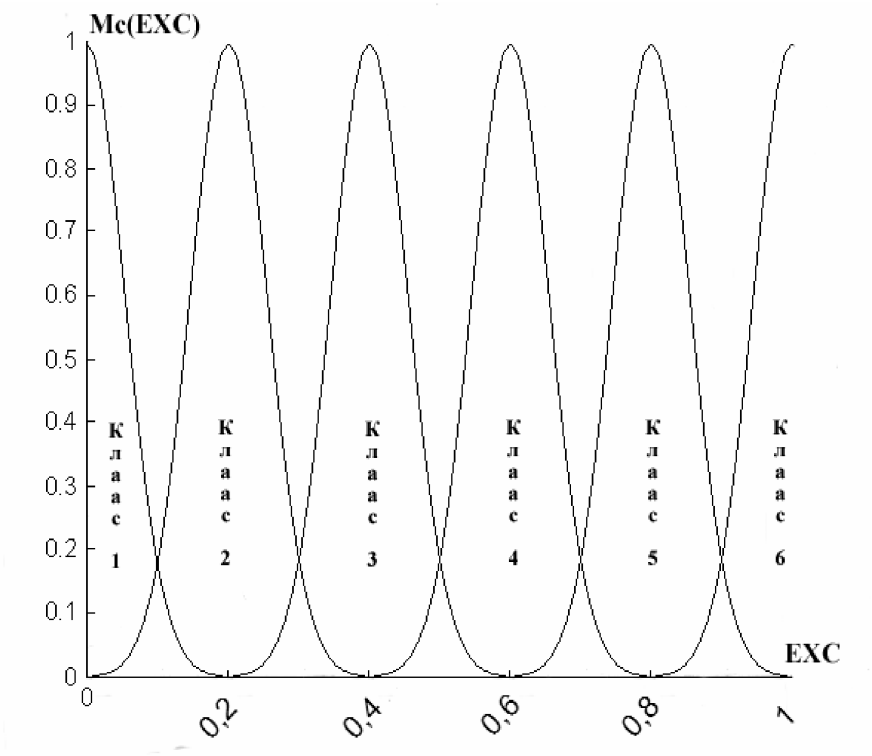


Рис. 4.8. Совокупность кривых принадлежности для всех классов

Теперь по полученному нами значению единой характеристики конфликта EXC и по функциям принадлежности каждого класса, определим, к какому классу и с какой степенью принадлежит конфликт, т.е. мы получим определяющую фазу конфликта.

4.2.5. Метод определения сценария дальнейшего развития международного конфликта

Под *сценарием* понимается множество факторов, соответствующих событиям, которые могут произойти в прогнозируемый период.

Для его определения используется архив статистических данных по конфликтам, хранящий информацию о прошедших конфликтах, и данные о состоянии исследуемого конфликта в соответствии со структурой (рис. 4.9.).

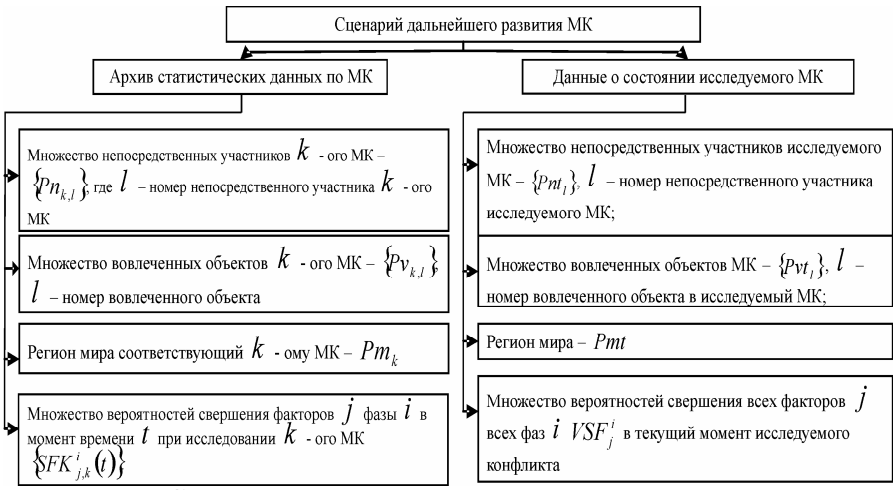


Рис. 4.9. Структура архива статистических данных и данных об исследуемом конфликте

Определение сценария дальнейшего развития межгосударственного конфликта осуществляется с использованием метода мягких притязаний в три этапа.

1) Определение степени близости состояний исследуемого МК и конфликтов из архива статистических данных. Для этого необходимо последовательно выбирать конфликты из архива статистических данных по МК и определять степень близости параметров исследуемого МК и параметров выбранного конфликта:

Степень близости непосредственных участников конфликта, вычисляется, как отношение количества совпадающих непосредственных участников конфликта и общее количество непосредственных участников.

$$Psn_k = \frac{Chn_k}{Cun_k} \tag{21}$$

где $Chn_k = \left|\{Pnt_l\} \cap \{Pn_{k,l}\}\right|$ - количество совпавших непосредственных участников, $Cun_k = \left|\{Pnt_l\} \cup \{Pn_{k,l}\}\right|$ - общее количество непосредственных участников.

Степень близости вовлеченных объектов вычисляется аналогично.

$$Psv_k = \frac{Chv_k}{Cuv_k} \tag{22}$$

где $Chv_k = \left|\{Pvt_l\} \cap \{Pv_{k,l}\}\right|$ - количество совпавших вовлеченных объектов, $Cuv_k = \left|\{Pvt_l\} \cup \{Pv_{k,l}\}\right|$ - общее количество вовлеченных объектов.

Степень совпадения региона мира представляет собой пороговую функцию.

$$Psm_k = \begin{cases} 0.1, \textit{если } Pmt \neq Pm_k \\ Pkm, \textit{если } Pmt = Pm_k \end{cases} \tag{23}$$

где Psm_k - Степень совпадения регионов мира, Pkm - значимость признака, показывающая важность совпадения регионов мира, в которых происходили МК.

Далее рассчитанные вероятности свершения всех факторов исследуемого конфликта необходимо сравнить с вероятностями свершения этих же факторов каждого конфликта из архива статистических данных. Относительное отклонение вероятностей свершения факторов вычисляется как сумма мер удаленности вероятностей свершения факторов исследуемого конфликта и конфликта, выбранного из архива статистических данных.

$$SKR_k(t) = \sum_{i=1}^{CFz} \sum_{j=1}^{CF^i} \begin{cases} \dfrac{\left|SFK^i_{j,k}(t) - VSF^i_j\right|}{SFK^i_{j,\max}(t) - VSF^i_j}; SFK^i_{j,k}(t) > VSF^i_j \\ \dfrac{\left|SFK^i_{j,k}(t) - VSF^i_j\right|}{VSF^i_j - SFK^i_{j,\min}(t)}; SFK^i_{j,k}(t) < VSF^i_j \end{cases} \quad (24)$$

где $CFz = 6$ - количество фаз, CF^i - количество факторов описывающих I-ую фазу.

Степень близости состояний исследуемого конфликта и конфликтов из архива статистических данных определяется на основании относительного отклонения вероятностей свершения факторов с учетом степеней совпадения непосредственных участников, вовлеченных объектов и региона мира.

$$Scc_k(t) = Pkn * Psn_k + Pkv * Psv_k + Psm_k + SKR_k(t) \quad (25)$$

Где Pkn - значимость признака, отражающая важность совпадения непосредственных участников конфликта, Pkv - значимость признака, отражающая важность совпадения вовлеченных объектов.

2) Эксперт определяет пороговое значение близости состояний. Далее определяем множество состояний конфликтов из архива статистических данных, которые являются близкими к текущему состоянию исследуемого конфликта.

$$Chc(k,t) = \left\{k,t \middle| Scc_k(t) \le Csp\right\} \quad (26)$$

где Csp - пороговое значение близости, $Chc(k,t)$ - множество состояний конфликтов из архива статистических данных близких к текущему состоянию исследуемого конфликта.

3) Факторы, свершившиеся в отобранных состояниях конфликтов из архива статистических данных в прогнозируемый период времени, и являются факторами возможного сценария дальнейшего развития исследуемого конфликта. Показатель свершения каждого фактора сценария вычисляется как средняя вероятность свершения

этого фактора по полученным состояниям отобранных конфликтов в прогнозируемый промежуток времени.

$$SFK^{i}_{jk}(\Delta t) = \frac{\sum_{t} SFK^{i}_{jk}(t)}{\Delta t} \tag{27}$$

где Δt - количество дней прогноза, t из Δt, $SFK^{i}_{jk}(\Delta t)$ - показатель свершения j-ого фактора i-ой фазы в k-ой конфликте за Δt, $SFK^{i}_{jk}(t)$ - показатели свершения факторов j фазы i в момент времени t при исследовании k-ого МК.

$$VSF^{i}_{j}(\Delta t) = \frac{\sum_{kt} SFK^{i}_{jk}(\Delta t)}{\left|Chc(k,t)\right|} \tag{28}$$

где $(k,t) \in Chc(k,t)$, $VSF^{i}_{j}(\Delta t)$ - показатель свершения фактора сценария j фазы i в прогнозируемый интервал времени Δt.

4.2.6. Описание методики компьютерного прогнозирования развития международного конфликта

Прогнозирование развития МК осуществляется с использованием представленной фазово-факторной модели путем расчета определяющей фазы и сценария дальнейшего его развития на прогнозируемый период[81].

Для прогнозирования МК используются следующие базы данных (рис. 4.10.):

[81] Кретов В.С., Котов М.Н. Компьютерное прогнозирование развития межгосударственного конфликта // «Проблемы управления безопасностью сложных систем». Труды XVII Международной конференции, декабрь 2009г; под ред. Н.И.Архиповой, В.В.Кульбы. М.:РГГУ, 2009

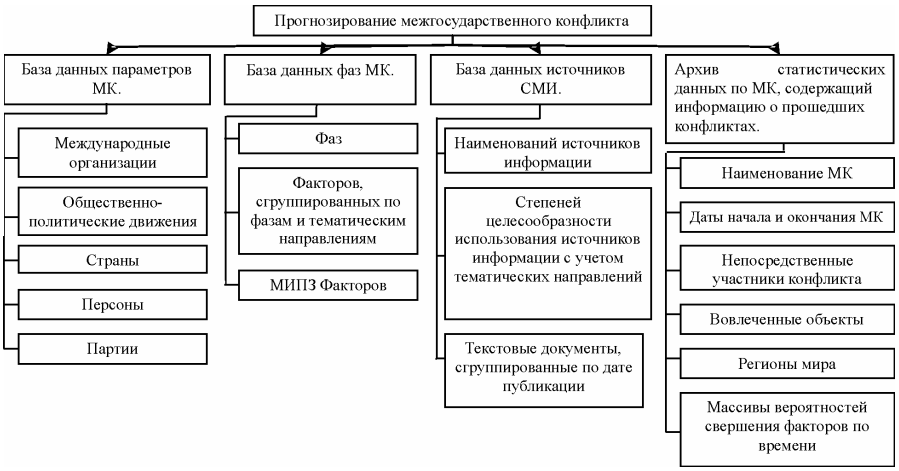


Рис. 4.10. Базы данных, используемые для прогнозирования развития межгосударственного конфликта

Блок-схема компьютерного прогнозирования направлений развития МК представлена на рис. 4.11.

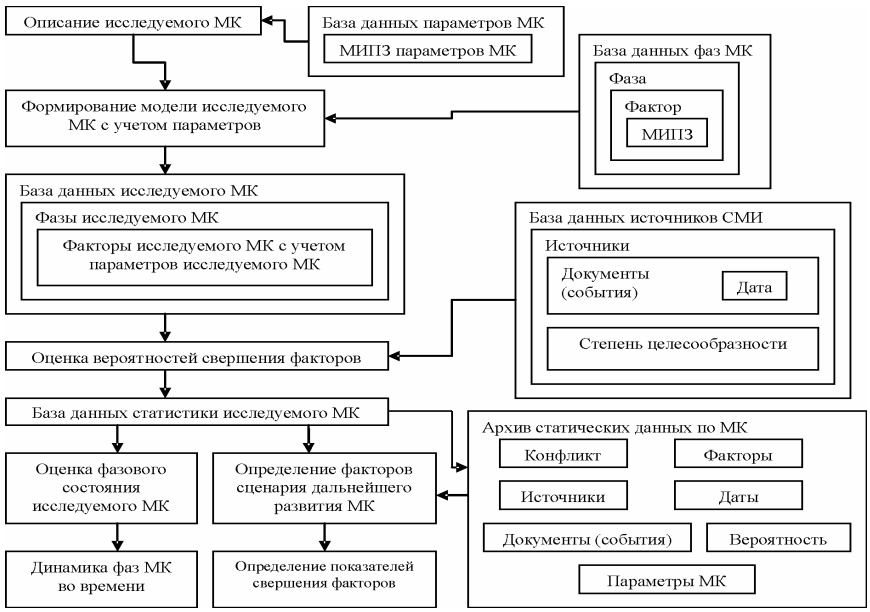


Рис. 4.11. Блок-схема компьютерного прогнозирования направлений развития МК

Согласно этой блок-схеме прогнозирование направлений развития МК включает следующие этапы:

1) Описание исследуемого конфликта.

Для этого вводим идентифицирующую информацию об исследуемом конфликте:

- Название МК;
- Дата начала исследования конфликта;
- Дата окончания исследования конфликта (при наличии).

Затем из базы данных параметров конфликтов выбираем параметры, соответствующие исследуемому конфликту. Параметрами исследуемого конфликта являются:

- Непосредственные участники конфликта;
- Вовлеченные объекты (общественно-политические движения, международные организации, партии, персоны, третьи страны);
- Регионы мира.

2) Формирование модели исследуемого МК с учетом параметров.

Для этого программно адаптируем параметрическую фазово-факторную модель МК из базы данных фаз конфликтов с учетом параметров, используемых при описании исследуемого конфликта. В результате будет создана база данных исследуемого конфликта.

3) Оценка вероятностей свершения факторов (на основании разработанного метода).

Для этого необходимо вычислить цитируемость факторов, применяя к информации, полученной из базы данных источников СМИ в исследуемый период, МИПЗ с параметрами, определяющими исследуемый конфликт.

4) Пополнение базы данных статистики исследуемого МК оценками вероятностей свершения факторов.

5) Пополнение архива статических данных по конфликтам оценками вероятностей свершения факторов исследуемого конфликта.

6) Оценка фазового состояния исследуемого МК (на основании разработанного метода) - определение динамики фаз во времени.

7) Определение показателей свершения факторов сценария дальнейшего развития МК на прогнозируемый период на основании метода, описанного выше, с использованием информации архива статистических данных по конфликтам и базы данных статистики МК.

Использование данной методики позволяет исследовать МК как динамический, многосторонний и сложный процесс. **В связи с тем,**

что методика подразумевает участие эксперта только на стадии обучения системы, появляется возможность оперативно выполнять анализ и прогнозировать развитие конфликта на заданный промежуток времени.

4.3. Программная реализация методики прогнозирования направлений развития международного конфликта

Программная реализация методики представляет собой специальный программный комплекс, функционирующий совместно с интеллектуальной ИПС «Истра-2006».

В методике прогнозирования направлений развития МК используются следующие возможности ИПС «Истра-2006»:

- Ведение БД Интернет-источников СМИ;
- Ведение БД иерархической системы моделей информационно-поисковых запросов;
- Ведение БД статистики появления текстовых сообщений СМИ в банке данных ИАС.

На рисунке 4.12. представлена схема интеграции специального программного комплекса, разработанного для реализации предлагаемой методики прогнозирования направлений развития МК, с ИПС «Истра-2006».

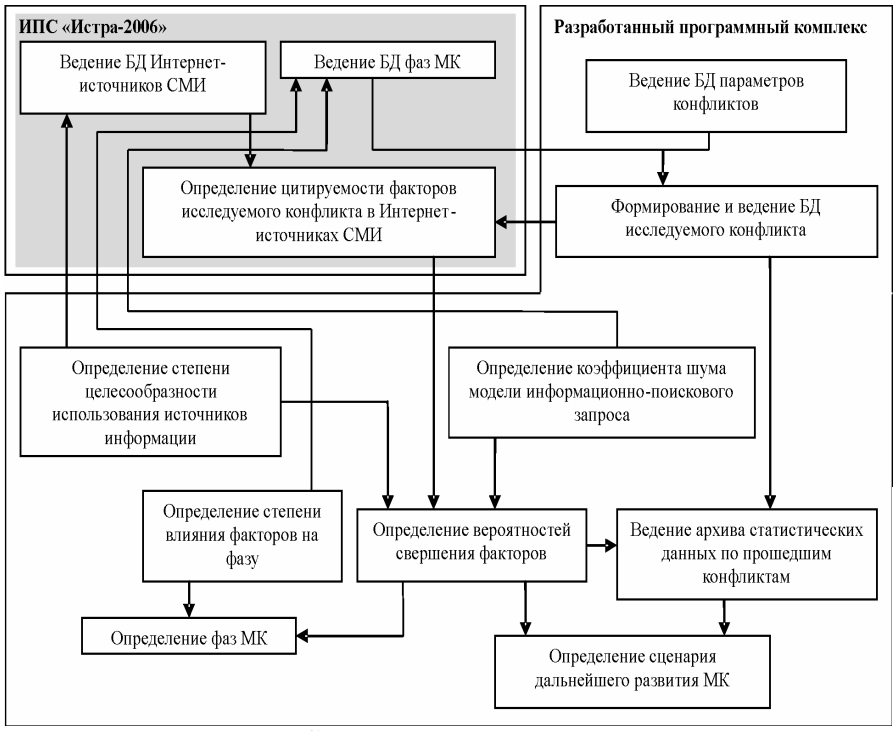


Рис. 4.12. Схема интеграции специального программного комплекса и ИПС «Истра-2006»

ИПС «Истра-2006» используется для ведения БД Интернет-источников СМИ и БД фаз конфликтов. Комплекс осуществляет ведение БД параметров конфликтов, а также формирует и ведет БД исследуемого МК при помощи программной адаптации фазово-факторной модели из БД фаз МК с учетом его параметров. На основании информации из БД исследуемого МК и БД Интернет-источников СМИ ИАС «Истра» определяет цитируемость факторов МК в Интернет-источниках СМИ.

Комплекс определяет степени целесообразности использования источников информации и коэффициенты шума моделей информационно-поискового запроса, которыми пополняет БД Интернет-источников СМИ и БД фаз МК. На основании полученных параметров с учетом цитируемости факторов МК программный комплекс вычисляет вероятности свершения факторов. Кроме того, разработанный комплекс определяет степени влияния факторов на соответствующую фазу и на их основании с учетом вероятностей свершения факторов определяет фазу конфликта.

После того, как БД исследуемого конфликта сформирована и пополнена значениями вероятностей свершения факторов, разработанный программный комплекс пополняет ими архив статистических данных по прошедшим конфликтам. Далее на основании архива статданных и вероятностей свершения факторов определяется сценарий дальнейшего развития МК.

Предложенная методика компьютерного прогнозирования развития МК реализована в технологии «клиент-сервер» в виде программы, написанной на четырех языках: Java Script, Basic Script, язык разметки HTML, язык запросов к БД SQL. БД реализована в Microsoft Office Access 2003.

Работа программного комплекса была проверена на операции «Литой свинец» (кодовое название боевых действий между Израилем и террористической группировкой ХАМАС), проходившей с 27 декабря 2008 г. по 18 января 2009 г. на территории Сектора Газа. Определение сценария дальнейшего развития операции «Литой свинец» проводилось с 01.01.2009 г. на 4 дня.

В результате проведенного сравнительного анализа результатов работы комплекса и событий, реально произошедших в ходе операции «Литой свинец» в прогнозируемый период времени, было выявлено, что точность прогноза составила 60%. **Программный комплекс позволил правильно выявить 8 из 11 событий, которые произошли в операции «Литой свинец» в прогнозируемый период времени**.

Таким образом, для решения актуальной научной задачи прогнозирования направлений развития международных конфликтов разработана инновационная компьютерная методика, включающая в себя пять взаимоувязанных частных прикладных научных методов и программную реализацию в виде специального программного комплекса, интегрированного с ИПС «Истра-2006. Проведена апробация методики, показавшая ее работоспособность.

4.4. Информационно-аналитические программные комплексы Института экономических стратегий (ИНЭС) - поддержка принятия решений в сфере международных отношений

Хронологически первым программным комплексом ИНЭС, нацеленным на моделирование возможных изменений в системе международных отношений, стала экспертно-моделирующая система - программный комплекс «Баланс интересов», разработанный по заказу МИД России и при внедрении (2001 г.) получивший название

«Смоленка». Данный комплекс используется в структурных подразделениях МИД для анализа систем интересов, выявления противоречий в межгосударственных отношениях стран Ближнего Востока, а также в Закавказье (рис. 4.13.).

Рис. 4.13. Основные функции программного комплекса «Баланс интересов» («Смоленка»)

Некоторые результаты исследования систем интересов государств Закавказья и крупных внерегиональных держав, оказывающих воздействие на формирование обстановки в регионе, прогноз возможных трансформаций этих интересов в соответствии с основными сценариями были ранее опубликованы. Исходя из этого, основное внимание сконцентрируем на другом программном продукте Института экономических стратегий - ПК «Стратегическая матрица России», который стал первым в новой серии программных комплексов, объединенных проектом «Стратегическая матрица».

Стратегическая матрица государства формируется на основе методологии многофакторного анализа, которая обеспечивает принятие стратегических решений высшим политическим руководством страны на базе учета существующих исторических закономерностей, позитивного и негативного опыта отечественной и мировой истории (рис. 4.14.).

Рис. 4.14. Возможности программного комплекса «Стратегическая матрица государства»

В 2004 г. усилиями коллектива Института экономических стратегий выпущены две основополагающие книги[82], одна из которых «Россия в пространстве и времени» признана Российской государственной библиотекой лучшей книгой 2004 г. в разделе «Политология». Впоследствии авторы выпустили целую серию книг и публикаций, результаты которых базировались на методологии «Стратегической матрицы»[83].

[82] А.И.Агеев, Б.В.Куроедов, О.В.Сандаров Методология стратегической матрицы. М.: ИНЭС, 2004
Б.Н. Кузык, А.И. Агеев, О.В.Доброчеев, Б.В. Куроедов, Б.А. Мясоедов. Россия в пространстве и времени. М.: ИНЭС, 2004

[83] А.И.Агеев, Б.В.Куроедов. Стратегическая матрица Казахстана. М.: ИНЭС, 2005
А.И.Агеев, Б.В.Куроедов. Стратегическая матрица Украины. М.: ИНЭС, 2005
А.И.Агеев, С.П.Головаченко, Б.В.Куроедов. Стратегическая матрица Беларуси. М.: ИНЭС, 2005
А.И.Агеев, А.Байшуаков, Б.В.Куроедов. Стратегическая матрица Казахстана. 2-е издание, дополненное и переработанное. М.: ИНЭС, 2006
А.И.Агеев, А.Г.Апостолов, Б.В. Куроедов. Стратегическая матрица Болгарии от древнейших времен до середины XXI века. М.: ИНЭС, 2006
А.И.Агеев, Б.В.Куроедов. Особенности применения методологии «Стратегической матрицы» при прогнозировании перспектив развития государств (на примере России и Китая). М.: ИНЭС, 2006
А.И.Агеев, Б.В.Куроедов. Особенности применения методологии «Стратегической матрицы» при прогнозировании перспектив развития государств (на примере России и Китая). 2-е издание. М.: ИНЭС, 2008

Начиная с 2007 г., метод «Стратегической матрицы» был модифицирован для решения прикладной задачи оценки и прогноза изменения интегральных показателей мощи государств[84]. На этом этапе авторам удалось решить задачу сопоставления потенциалов различных государств и их реализованной мощи в конкретный момент времени (рис. 4.15.). Мощь западноевропейских стран рассматривалась как в составе ЕС, так и на национальном уровне.

РЕЙТИНГ В НАСТОЯЩЕЕ ВРЕМЯ	ГОСУДАРСТВО	РЕЙТИНГ В 2025 Г. (СЦЕНАРИЙ «УМЕРЕННАЯ ГЛОБАЛИЗАЦИЯ»)	ИЗМЕНЕНИЕ РЕЙТИНГА
1	США	1	●
2	ЕС	2	●
3	Китай	3	●
4	Россия	4	●
5	Германия	6	▼
6	Франция	9	▼
7	Великобритания	8	▼
8	Индия	5	▲
9	Япония	10	▼
10	Бразилия	7	▲

Рис. 4.15. Прогноз изменения рейтинга 10 ведущих стран мира в период до 2025 г.

Следует отметить, что сама идея построения стратегической матрицы многофакторного анализа базируется на постулате, что развитие страны (государства) происходит под влиянием набора факторов, каждый из которых оказывает разноплановое воздействие на большую систему, которую представляет собой государство. Все эти факторы классифицированы путем их сведения в большие группы, каждая из которых условно представлена в виде одного фактора, который в модели стратегической матрицы отражает совокупное влияние на развитие системы всех факторов, относимых к данной группе.

Хотя воздействие факторов постоянно видоизменяется, для представления результатов исследования в конкретной временной точке используются их статические значения в конкретный период времени, которые оцениваются при помощи специально разработанных критериальных шкал.

[84] Глобальный рейтинг интегральной мощи 50 ведущих стран мира. Доклад к обсуждению. М.: МЛСУ, МАИБ, ИНЭС, 2007
Глобальный рейтинг интегральной мощи 100 ведущих стран мира. Доклад к обсуждению. М.: МЛСУ, МАИБ, ИНЭС, 2008

Статистический подход преобладает при определении значений факторов «Территория», «Население» и, частично, «Экономика», для остальных параметров используется вычисление на основе обобщенных экспертных оценок. В этом случае факторы описываются рядом частных параметров, количество (как правило, в диапазоне 4-10) и относительная важность которых могут варьироваться для различных исторических или прогнозных временных рубежей.

Их значения соотносятся со специальными критериальными шкалами, которые определяют верхний, средний и нижний уровни развития государства в диапазонах «сверхдержава», «великая держава», «региональная держава», а также низший уровень - «малое государство».

Значения факторов, описывающих территорию, природные ресурсы, население, культуру и религию, определяют потенциал развития государства. Другая группа - факторы, отражающие реализацию имеющегося потенциала; экономика, наука и образование, армия и внешняя политика (рис. 4.16.).

Фактор «Управления» венчает конструкцию многофакторного анализа, поскольку именно управление провоцирует изменчивость всей системы в целом, оценка качества управления является одной из наиболее динамично меняющихся характеристик, что во многом объясняется существенными субъективными воздействиями на нее.

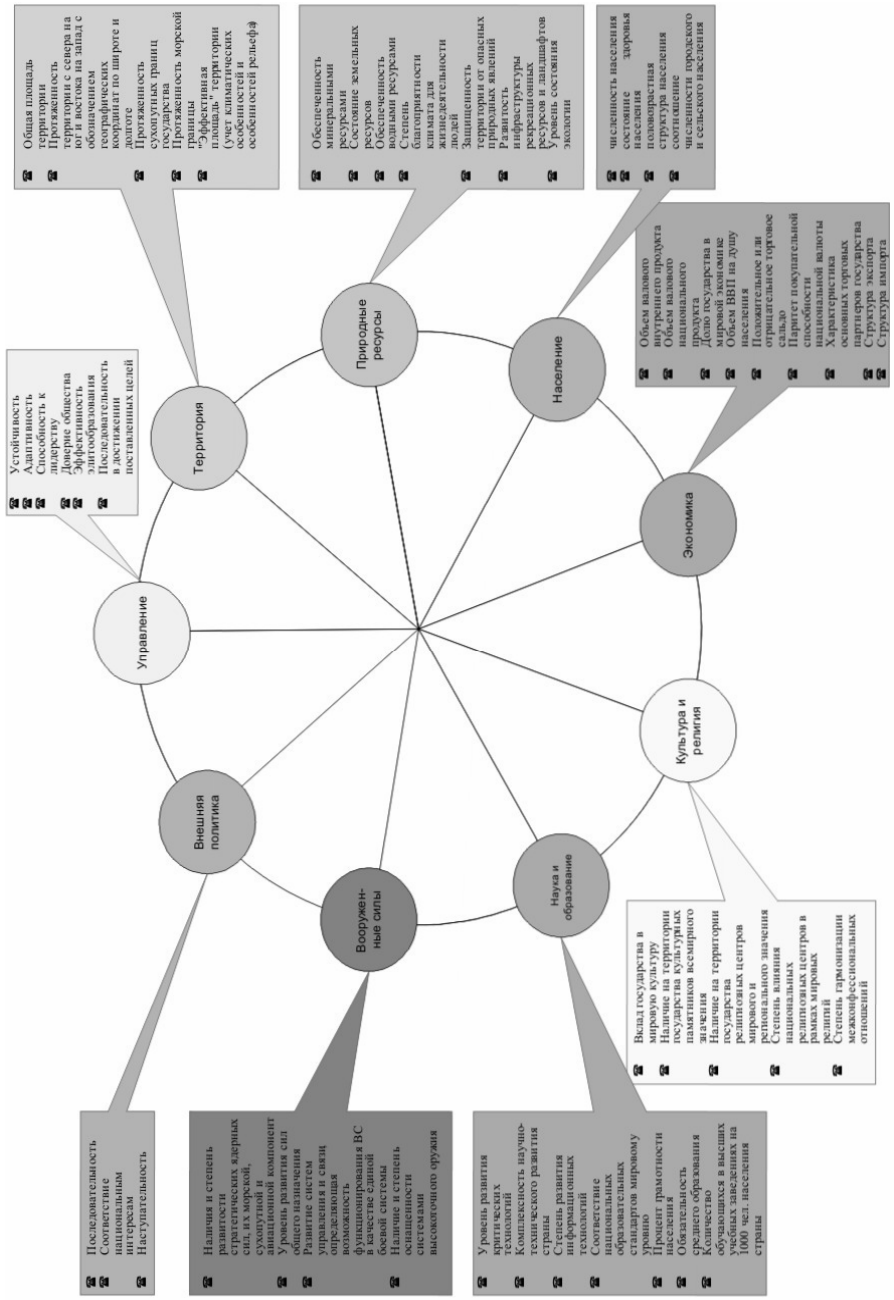


Рис. 4.16. Основные показатели, используемые для описания уровня развития государства

Применение методологии «Стратегической матрицы» на базе ПК «Стратегическая матрица России» также было апробировано в совместном докладе ИНЭС и Международной академии исследования будущего «Россия и мир: взгляд из 2017 года»[85].

Проведенные исследования показали, что позиции России в современной системе международных отношений обусловлены тем, что, с одной стороны, она пока не располагает достаточными экономическими и демографическими возможностями, чтобы претендовать на роль самостоятельного мирового центра силы (рис. 4.17.). С другой - сохраняющиеся военные возможности России (особенно в сфере ракетно-ядерных вооружений), научный и промышленный потенциал (например, помимо США только Россия в состоянии сегодня самостоятельно производить весь спектр современного вооружения и военной техники), безусловно, определяют ее уникальную роль на мировой арене.

Огрублено, суть сегодняшней развилки в развитии страны исчерпывающе описывается тремя цифрами: 6; 7,5; 2,3. За ними - тот непреложный факт, что в зависимости от качества стратегических решений, которые будут приниматься государством, бизнесом, обществом в настоящее время, мы, как страна, можем либо подняться до устойчивого положения сбалансированной великой державы вплотную приблизившись к статусу сверхдержавы (7,5 баллов), либо скатиться на уровень третьестепенного регионально значимого государства (2,3 балла), а, не исключено, некоторого множества государств.

Россия в состоянии сформировать один из весомых центров силы современного мира путем заключения двусторонних и многосторонних договоров со странами ближнего зарубежья. Поэтому **стратегической целью России должна стать экономическая и военно-политическая интеграция постсоветского пространства.**

В целом позитивный для России сценарий развития международных отношений должен строиться исходя из следующих условий:

1. Внешняя политика является весьма зависимым фактором от других параметров мощи государства - прежде всего от факторов управления, экономики и уровня развития вооруженных сил.

В то же время успешная или провальная внешняя политика формирует условия функционирования государства в благоприятной или неблагоприятной внешней среде, что оказывает сущест-

[85] А.И.Агеев и др. Россия и мир: взгляд из 2017 года. М.: ИНЭС, 2007

венное воздействие на формирование всех остальных факторов мощи государства.

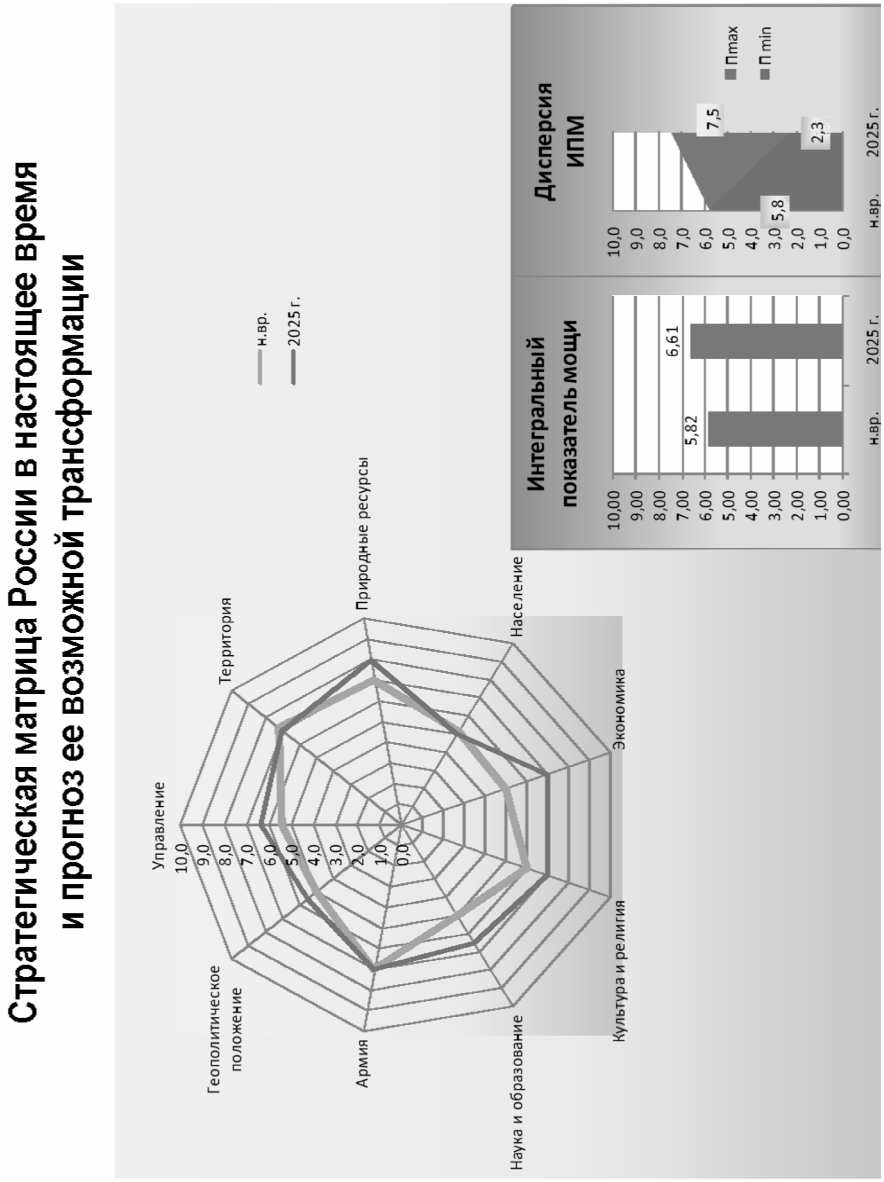


Рис. 4.17. Стратегическая матрица России в настоящее время и прогноз ее возможной трансформации

2. Утрата Россией сверхдержавного статуса в исторически недавнем прошлом на прогнозируемый период до 2017 г. оставляет открытым вопрос о ее дальнейшем внешнеполитическом статусе, что подразумевает как возможности дальнейшей утраты внешнеполитического влияния, так и возможности, наоборот, усиления внешней политики страны.

3. На ближайшую перспективу внешнеполитическое положение России будет определяться, с одной стороны, отсутствием явной конфронтации во взаимоотношениях с ведущими мировыми центрами силы, с другой - активным геополитическим наступлением стран евроатлантического сообщества на интересы России, в том числе на наиболее чувствительном для нее постсоветском пространстве.

4. Отсутствие в ближайшем геополитическом окружении России сильных союзников и надежных стратегических партнеров придает ее внешнеполитическому положению существенную степень неустойчивости.

5. Отмечается возрастание значимости нетрадиционных угроз интересам национальной безопасности, прежде всего со стороны сетевых террористических структур, а также организованной преступности, опасности техногенных катастроф и т.д.

Россия снова сталкивается с необходимостью мобилизации, нового рывка, чтобы отстоять свою безопасность и удовлетворить возросшие за период релаксации социальные ожидания.

Единственно приемлемый в этих условиях вариант инновационного прорыва, способный оптимальным способом поменять экономическую структуру страны, выведя ее в разряд развитых постиндустриальных государств, потребует мобилизации творческого потенциала нации, обеспечивающего гармоничное сочетание всех факторов развития государства.

Главным условием успешного решения задач обеспечения инновационного прорыва является построение эффективной системы управления, настроенной на решение задач стратегического предвидения, а не на бесперспективное реагирования на «внезапно возникающие ситуации». Однако за всяким государственным аппаратом всегда стоит социальная элита.

Назрело существенное обновление правящей элиты. Новая элита, не отягощенная враждой с обществом, должна реализовать эффективное изменение социально-экономического курса. Строго говоря, смена элит произойдет в ближайшие 5-10 лет неизбежно, повинуясь закону смены поколений. В любом случае в

2010-2015 гг. мы увидим иные действующие лица среди научного, культурного, делового, военного, политического сообществ России.

Для реализации процесса элитообразования необходимо создать социальные «лифты» (задача, которая решалась в России в эпохи преобразований Петра, и после опустошительной гражданской войны), сформировать кадровые резервы, активировать смены с выводом из управленческого оборота дискредитировавших себя деятелей вместо осуществления бесплодных перестановок.

Стратегической, жизненно важной задачей является преодоление демографического кризиса. При худших вариантах развития ситуации к 2080 г. Россия может приблизиться к катастрофическому уровню численности населения страны в 50-60 млн.чел. При таком развитии событий невозможно всерьез говорить не только о решении задачи сохранения за Россией статуса одного из центров мировой цивилизации, но даже о перспективах сохранения российской государственности как таковой.

Решение демографической проблемы во многом связано с повышением социальной энергетики нации, которой необходим жизнеутверждающий импульс.

Основой этого жизнеутверждающего импульса должно стать успешное духовное и экономическое развитие с опорой на развитие высокотехнологичных отраслей промышленности, базирующихся на ультрасовременных прорывных технологиях. Обеспечить этот прорывной технологический уровень в состоянии только современная и высокоэффективная система образования и утверждение высоких культурных стандартов жизни в изменившемся мире.

Усилению энергетики нации и конкурентоспособности отечественной экономики способствовало бы усиление центростремительных тенденций на постсоветском пространстве. На фоне общемировой тенденции формирования крупных экономических мегаблоков, реинтеграция России и ее традиционных партнеров на евроазиатском пространстве - необходимое условие успешной реализации их геоэкономических интересов в условиях нарастающей глобализации мировой экономики.

Не менее важной задачей является консолидация общества на основе взаимоуважительного отношения традиционных религий и культурных особенностей различных конфессиональных и национальных групп. Консолидация российского общества должна подготовить его к противодействию все более сложным глобальным вызовам, таким как международный терроризм, организованная преступность, экологические вызовы и климатические изменения.

Поддержание боеспособных вооруженных сил на уровне оборонной достаточности - одно из основных условий формирования благоприятной внешнеполитической обстановки для реализации инновационного прорыва. При этом потенциал инновационного развития должен быть реализован в том числе и в направлении повышения обороноспособности страны, поиска и реализации прорывных решений по удешевлению поддержания вооруженных сил на уровне оборонной достаточности при одновременном существенном повышении их эффективности.

Уверенная внешняя политика, обеспечивающая реализацию жизненно важных интересов государства в геополитической и геоэкономической сферах, - удел сильных в экономическом и военном отношении государств с выстроенной высокоэффективной системой управления.

Таким образом, первым и главным шагом на пути реализации инновационного прорыва должно стать построение государственного управления на принципах стратегического предвидения, учета всех условий совершения страной крупномасштабного прорыва в развитии.

Целью же данной работы - формирование основ инструментария стратегического планирования, посильная подготовка лиц, ответственных за судьбу страны, к быстрому и обоснованному принятию решений в интересах российского общества в условиях быстроменяющейся обстановки, формирование инновационного мышления у людей, причастных к государственному управлению. Одновременно эта работа является вкладом в широкую пропаганду консолидации российского общества вокруг идеи инновационного прорыва России в XXI веке как единственного эффективного пути культурного, национального, экономического и геополитического возрождения и развития нашей страны в жестких условиях современных цивилизационных вызовов.

В целом, использование **методологии «Стратегической матрицы»** достаточно наглядно демонстрирует возможные альтернативы развития России в XXI веке. При этом спектр возможного стратегического выбора для нее достаточно широк. Россия пока еще сохраняет шансы восстановить позиции одного из мировых лидеров, но, хотя ей и удалось отойти от края пропасти, за которым стоял развал страны и лилипутизация ее осколков, при определенных условиях подобный сценарий может стать для нее реальностью. В чем же состоит содержание основных стратегических альтернатив для России в XXI веке?

Евразийская интеграция оставляет России возможность вернуться к «сверхдержавному статусу», который будет принадлежать ей не единолично, а как одному из элементов (хотя и наиболее крупному) в конструкции Евразийского пространства.

Как уже отмечалось выше, при реализации данной стратегии Евразийскому пространству (конфигурации которого могут быть различны) практически предстоит пройти путь, во многом сходный тому, который был пройден Евросоюзом.

Поскольку основой Евразийской интеграции скорее всего или даже исключительно могут стать постсоветские государства, то это, с одной стороны, облегчает построение интеграционных связей, но, с другой, требует преодоления ими психологического груза боязни утраты недавно обретенной независимости. Ясно, что помимо психологических факторов свою роль сыграют и мотивы сугубо внутриполитические.

Особенность данной стратегии состоит в том, что ее реализация требует сжатых сроков, поскольку в условиях обостряющейся борьбы мировых центров силы за «советское наследство» существует определенная временная «линия смерти», пройдя которую об ускоренной реинтеграции Евразийского пространства говорить будет сложно. Этот временной отрезок, скорее всего, можно связать с приходом к власти в постсоветских государствах нового поколения, сформировавшегося уже после развала СССР. Т.е. к дате развала Советского Союза необходимо прибавить примерно 25-30 лет, и мы определим этот рубеж на уровне 2015-2020 годов, т.е. избранный нами прогнозный горизонт 2017 года как раз приходится на середину этого отрезка.

Способна ли за оставшиеся 7-10 лет какая-то часть постсоветского пространства, которая еще не поглощена экспансией ЕС и НАТО, самоорганизоваться и осуществить прорыв в формировании Евразийского союза? Наметившаяся положительная динамика в формировании ОДКБ и Таможенного союза внушает некоторый оптимизм. Однако темпы их развития явно недостаточны.

Очевидно, что идея интегрирования евразийского пространства наталкивается на сильное противодействие как внутри стран постсоветского пространства, так и вне его. Ни один из существующих мировых центров силы не заинтересован в появлении равнозначного или сопоставимого с ним по мощи игрока на международной арене. Именно поэтому продолжается процесс экспансии европейских и евроатлантических структур на постсоветском пространстве.

Перспективы формирования Евразийского пространства по отдельным элементам модели «Стратегической матрицы» представляются следующим образом.

«Управление». Наиболее эффективной базой для формирования наднациональных институтов представляется наличие эффективных демократий в государствах постсоветского пространства. Вместе с тем реальная ситуация в этих государствах такова, что характерная для большинства из них та или иная форма монопартийности при сильном лидере государства создает сходный политический ландшафт, что может быть использовано на первом этапе формирования Евразийского союза как дополнительный ресурс.

В дальнейшем сама логика развития интеграционного объединения потребует развития демократических институтов и формирования благоприятной среды для конкуренции идей. Т.е. необходимость построения эффективной системы управления наднационального уровня будет подстегивать развитие демократических институтов сначала на наднациональном уровне, что будет в дальнейшем проецироваться на национальные политические системы государств-участниц.

Против Евразийской интеграции выступает и незавершенность политических процессов внутри России. Ее политический класс поглощен внутриполитической борьбой и пока не в полной мере готов решать сложные стратегические задачи по реинтеграции постсоветского пространства.

«Территория». Пространственный облик возможного Евразийского союза достаточно расплывчат. Украина или какая-то ее часть еще имеет шанс стать одним из системообразующих элементов Евразийского пространства, однако «зацикленность» значительной части украинской элиты, даже относительно лояльной к России ее части, на «европейском» выборе будет тормозить движение Украины в направлении евроазиатской интеграции.

Беларусь, теоретически наиболее продвинутая в отношении интеграции с Россией, на самом деле явно притормаживает свое движение к объединению с Россией. В силу чрезмерных личных амбиций руководства страны государство по численности населения и экономическому потенциалу сравнимое с отдельными регионами РФ претендует на равный с ней статус в межгосударственном объединении. Россия естественно не может пойти на это, так как такой подход не только может нарушить внутреннюю стабильность во взаимоотношениях Центра с регионами РФ, но и по той причине, что это окончательно подорвет идею широкой евразийской интеграции.

Вообще вопрос о статусе, а, еще вернее, о количестве голосов при принятии основополагающих решений интеграционного строительства отдельных государств в предполагаемом Евразийском союзе, возможно, главный на сегодняшний день.

Примером может служить ситуация с Казахстаном. По площади территории это второе после России государство. По численности населения оно вдвое больше Беларуси, однако вчетверо меньше Украины и почти в десять раз меньше России, более чем в полтора раза меньше, чем Узбекистан.

В то же время в экономическом плане Казахстан - лидер Центральной Азии, однако его экономический потенциал сопоставим с белорусским и существенно уступает украинскому.

Каким образом свести все эти показатели (численность населения, площадь территории, экономическая и финансовая мощь) в определении статуса и влияния отдельных государств-участников Евразийского союза? Формирование взаимоприемлемых для государств-участников критериев и формулы участия в управляющих органах Евразийского союза один из наиболее важных и сложных вопросов в отношении того, состоится или не состоится такой Союз в обозримом будущем.

При этом территориальные модели подобного союза могут носить как «европейский», так и «азиатский» уклон.

1. **«Славянская» интеграция**» Россия, Беларусь, Украина или ее часть. В суженном виде - Союзное государство России и Беларуси. При ее формировании решается вопрос разграничения России с ЕС в Европе, но открытым остается вопрос о влиянии мировых геополитических центров в Центральной Азии и Закавказье. Вариант, кажущийся легко реализуемым с точки зрения этнической и конфессиональной близости, однако именно в Украине и Беларуси Россия сталкивается с наиболее сильным и организованным внешним противодействием планам евразийской интеграции.

2. **«Россия плюс Центральная Азия»** за вычетом, может быть, Туркмении. Центральноазиатские государства сталкиваются с наиболее сильными вызовами собственной безопасности (угроза доминирования Китая, исламский фактор), в то же время Россия - государство с близкой ментальностью. Важный экономический и сильный в военном отношении партнер.

3. **«Славянская интеграция» плюс Центральная Азия**. На чаше плюсов уже отмеченное сходство менталитета, однако стратегические вызовы для европейских государств и стран Центральной Азии существенно различаются. Цементирующим узлом их объе-

динения может выступать только Россия, для которой актуален как европейский, так и центральноазиатский пакет вызовов и угроз.

4. Одна из наиболее внешне привлекательных моделей объединения - **«Славянский союз» плюс Казахстан**. В этой модели объединились бы наиболее развитые на постсоветском пространстве государства. В то же время экономические аутсайдеры СНГ окажутся вне процесса интеграции. Вряд ли это продуктивный вариант, поскольку экономический выигрыш скорее всего будет сопровождаться увеличением социального и военного напряжения на южных границах созданного в подобном формате союза.

Особый разговор о Закавказье, а также о Молдавии. Армения за счет союза с Россией решает задачу невмешательства Турции в ситуацию вокруг Нагорного Карабаха, однако при ее решении интерес к стратегическому партнерству с Россией будет слабеть. Вместе с тем скорого решения проблемы с НКР не предвидится, и поэтому сохранение ориентации Армении на Россию, по крайней мере, в сфере безопасности может сохраняться сколь угодно долго.

Практика построения крупных геополитических объединений (наиболее показателен в этом плане опыт Евросоюза), тем не менее, демонстрирует принцип географической приближенности, т.е. страна-кандидат должна иметь общую границу с другими государствами, входящими в интеграционное объединение. Армения же отделена от России и других стран – потенциальных участниц Грузией, втянутой в геополитическую орбиту Запада, и Азербайджаном, являющимся одной из сторон конфликта вокруг Нагорного Карабаха.

Примерно то же можно сказать и о Молдавии. В том случае, если Украина входит в евразийское поле интеграции, возможным становится и вовлечение в него Молдавии, в противном случае ее вхождение в процесс евразийской интеграции выглядит крайне проблематичным.

Таким образом, формирование Евразийского союза может происходить в первую очередь за счет стран, чья политическая элита и общество в наибольшей степени готовы пройти путь интеграционного развития. При этом доминирующим фактором, видимо, будет выступать **геополитическая целесообразность** и лишь на втором плане - экономическая составляющая. При формировании союза должны быть сформированы универсальные правила взаимодействия членов сообщества в рамках интеграционного объединения, предусматривающие возможность присоединения к нему в дальнейшем новых членов, которые по тем или иным причинам не готовы сделать это сегодня.

Природные ресурсы. Одна из причин, препятствующих реинтеграции постсоветского пространства, - схожие производственные возможности и конкуренция на европейских и мировых рынках, в том числе и в сырьевом компоненте. Так, Украина - один из наиболее крупных конкурентов России в сфере металлургии. Казахстан, Туркмения, Азербайджан и, в меньшей степени, Узбекистан конкурируют с Россией на рынке нефти и природного газа. Страны Закавказья (Азербайджан и Грузия) в предоставлении альтернативных, по отношению к российским, транспортных коридоров для доставки на европейский рынок нефти и газа из Центральной Азии. В принципе, большинство из этих разногласий преодолимо в процессе построения интеграционного объединения. За счет картельных соглашений и построения единой системы сырьевого экспорта участники этого рынка могут даже выиграть.

Против России играет то, что она слишком долго выступала донором за счет предоставления собственных энергетических ресурсов для постсоветских государств. Фактически Россия дотировала становление новых независимых государств, особенно, на западе европейской части СНГ и в Закавказье. Однако в настоящее время в стремлении перейти на рыночные механизмы формирования цен на энергоресурсы она ударилась в другую крайность, ставя на одну доску государства, сохраняющие стремление к интеграции с ней, и страны, чей геополитический выбор лежит вне поля евразийской интеграции. При этом необъяснимым образом преференции зачастую имеют государства, наиболее недружественные по отношению к России (страны Прибалтики и до недавнего времени - Грузия).

Демография. На фоне более чем миллиардного населения в Индии и Китае, рождения 300-миллионного жителя США, 460 млн. численности населения ЕС и демографического потенциала исламского мира, любое государство СНГ, включая Россию, в одиночку выглядит демографическим карликом. В то же время численность населения отдельных государств постсоветского пространства, например Украины или России, наряду с другими показателями, делает их слишком крупными для того, чтобы войти в состав уже существующих интеграционных объединений (ЕС). Все это сопровождается процессами депопуляции (отрицательными значениями роста численности населения) на постсоветском пространстве.

Таким образом, стремление преодолеть демографическую несостоятельность может стать одним из наиболее сильных побудительных мотивов к объединению, подобно тому, как это происходило в ЕС. Для России это, кроме всего прочего, возможность сформировать более ментально близкие миграционные потоки ра-

бочей силы из государств Центральной Азии, нежели приток рабочей силы из стран дальнего зарубежья.

Экономика. Преимущества крупных экономических систем по отношению к неинтегрированным национальным экономикам в условиях глобализирующегося мира очевидны и не требуют особых доказательств. Только экономически крупные субъекты (США, ЕС, Китай) в состоянии в полной мере обеспечивать собственные интересы в рамках ВТО, вести скрытые и открытые торговые войны со своими оппонентами.

Россия, кажется, нашла свою нишу в качестве крупного энергетического субъекта современного мира. Однако это очень однобокая ниша и, как показывает опыт СССР, опора только на сырьевую составляющую в мировой торговле делает страну весьма уязвимой к внешним воздействиям. К тому же в энергетической сфере лидерство России не является неоспоримым.

Развитие событий в 2006 г. вокруг приобретения российским банком пакета акций европейского авиационно-космического концерна EADS показывает нежелание западных партнеров пускать Россию на рынок высоких технологий развитых стран. Поэтому задача построения собственного высокотехнологичного комплекса крайне актуальна для России. Аналогичные задачи стоят и перед другими постсоветскими государствами. Однако их возможности в этой сфере еще более ограничены.

Поэтому объединение усилий для решения задач инновационного развития также один из побудительных мотивов создания единого **научного и образовательного** евразийского пространства.

Культура и религия. Более чем 70-летнее существование в рамках единого государства сформировало близкую ментальность проживавших на территории СССР народов. Несмотря на существенные религиозные и культурные различия, в целом фон культурного и межрелигиозного взаимодействия на постсоветском пространстве достаточно благоприятный.

Армия. Насущная необходимость координации усилий в военном строительстве демонстрируется успешным развитием интеграционных процессов в рамках ОДКБ, а также тем, что военное сотрудничество является, пожалуй, наиболее продвинутой и дееспособной сферой в рамках создания Союзного государства России и Беларуси.

Евразийское пространство, зажатое между военными гигантами современного мира Североатлантическим альянсом и Китаем, вынуждено искать пути достижения оборонной достаточности в отношениях с окружающим миром. Даже России, остающейся в воен-

ном измерении (во многом за счет ракетно-ядерного потенциала) мировой военной державой, в ближайшем будущем в связи с истощением мобилизационных запасов СССР, устареванием и деградацией военной техники из советского наследства решать эту задачу будет все сложнее. Наиболее приемлемый вариант - построение интегрированной системы обороны на евразийском пространстве с единым оборонно-промышленным комплексом, едиными стандартами вооружений и боевой подготовки.

Внешняя политика. Несмотря на наметившееся усиление влияния России в системе международных отношений, она попрежнему остается игроком второго уровня, уступая по степени своего влияния США и ЕС. Другие страны постсоветского пространства свою независимость в системе современных международных отношений зачастую реализуют путем выбора «сюзеренов». Яркий пример - Грузия, страны Прибалтики и т.д. Даже Украина - наиболее крупное государство постсоветского пространства - вынуждена балансировать между ЕС, НАТО и Россией в стремлении найти геополитическую опору для своего развития.

Формирование Евразийского союза - единственный вариант, в рамках которого небольшие страны постсоветского пространства в состоянии будут оказывать влияние на строительство мировой системы посредством своей субъектности в крупном геополитическом образовании. В противном случае они будут выступать объектами геополитических притязаний других субъектов.

При этом только Молдавия и, в более отдаленной перспективе, Беларусь могут представлять интерес в качестве новых членов других геополитических объединений (в данном случае имеется в виду ЕС).

Украина - слишком большое государственное образование, принятие которого в ЕС бросало бы вызов традиционным лидерам этой организации: Франции, Германии и Великобритании. Поэтому для нее возможной формой присоединения к евроатлантическим структурам являются разные формы углубленного партнерства, но не полноправное членство в ЕС (подобно тому, как это происходит в отношении Турции). Вопрос о возможности вступления Украины в НАТО оставим за скобками.

В целом выгоды интеграции Евразийского пространства для России очевидны. Только интеграционная постановка вопроса позволяет ей сохранять претензии на роль одного из мировых лидеров - «сверхдержаву XXI века».

Альтернативным проектом, имеющим много сторонников среди политической элиты России, является сохранение статуса «великой

державы» без углубленной интеграции постсоветского пространства. При всей привлекательности данного проекта, связанной с возможностью эгоистического поведения в сфере экономических взаимоотношений с государствами постсоветского пространства и возможностью балансирования между центрами силы мирового уровня, такая постановка вопроса представляется ошибочной. Ошибка заключается в механическом перенесении классического представления о великой державе из реалий XVI – начала XX века в XXI век с его глобализирующейся экономикой.

Субъектность на уровне современных международных отношений обеспечивается только за счет принадлежности к крупным торговым мегаблокам (ЕС, ССТ, МЕРКОСУР и т.д.) или для государств, имеющих сверхдержавный статус или приближающихся к нему (США, Китай). Однако даже для государств со статусом сверхдержав актуальным является построение собственных торгово-экономических блоков (ССТ\НАФТА для США, китаецентричной зоны свободной торговли в Восточной Азии для КНР).

Традиционные «великие державы», такие как Германия, Великобритания и Франция для сохранения своего влияния в системе международных отношений строят новое межгосударственное образование - ЕС.

Претендующая на статус «великой державы» Южной Америки Бразилия - один из инициаторов и наиболее активных участников общего рынка стран Южного конуса (МЕРКОСУР).

Уникальные ниши «великих держав» занимают сегодня, пожалуй, только Япония и Индия. Но это именно уникальные ниши особого геополитического расположения.

Япония, не сумев в полной мере реализовать свое финансовое могущество, все более проигрывает экономическое и геополитическое соревнование в Восточной Азии, набирающему влияние Китаю. Проигрывая демографически, не будучи в состоянии построить полноценные вооруженные силы и т.д., будущее Японии - превращение в достаточно мощную державу, но преимущественно регионального масштаба.

Индия, в силу особенностей своего геополитического положения -зажатости между региональными соперниками, превосходящими ее или сопоставимыми по мощи (Китаем и Пакистаном), - ограничена в своих возможностях построения собственной зоны влияния в Азии. Поэтому она не может в обозримом будущем претендовать на статус сверхдержавы и будет вынуждена и в дальнейшем выстраивать свое позиционирование в мире на основе баланса интересов с ведущими мировыми центрами силы.

В целом стратегия сохранения статус-кво «великой державы» для России представляется проигрышной. Она может на некоторое время заморозить на определенном уровне ее положение в системе экономических и геополитических взаимоотношений современного мира, но не оставляет России стратегической перспективы.

В условиях XXI века статус «великой державы» фактически может определяться только как транзитное состояние в движении к сверхдержавному статусу за счет построения собственного или на кооперативных началах торгово-экономического и военно-политического блоков. Другой альтернативой будет являться сползание к статусу региональной державы, что в условиях агрессивной внешней среды, в которой находится Россия, рано или поздно может означать отказ от ядерного статуса и значительные территориальные потери или даже утрату собственной государственности.

Таким образом, основой проекта «Стратегическая матрица» Института экономических стратегий (ИНЭС) является методология, которая обеспечивает проведение междисциплинарных исследований с использованием элементов теории нечеткой логики, теории графов, сценарного метода, метода анализа иерархий и других математических методов. Данная методология позволила сформировать единый инструментарий для проведения как ретроспективных, так и прогнозных исследований. Это повышает обоснованность прогнозов в отношении позиций отдельных субъектов в вопросах политического и военного блокирования, выбора ими своих внешнеполитических стратегий и приоритетов, связанных с объективным состоянием их международного окружения, потребности в союзниках и возможности объединения с другими субъектами международных отношений для защиты собственных интересов.

В целом следует отметить, что удалось решить крайне сложную задачу формализации и сведения в единую систему разноуровневой информации с высокой степенью нечеткости и неопределенности данных. Многочисленные публикации и доказанная возможность использования методологии для создания аналитических программных продуктов свидетельствуют о ее практической значимости.

Глава 5
ПРИКЛАДНЫЕ АСПЕКТЫ АНАЛИЗА ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ

Для успеха не надо быть намного умнее других, надо просто быть на день быстрее большинства.

Л.СЦИЛЛАРД

5.1. Арктика - «кухня» глобального политического климата

Распад СССР сместил геополитический центр России на Север, к Арктике. Как бы предчувствуя это, М.С.Горбачев в контексте философии нового политического мышления выдвинул 1 октября 1987 г. ряд инициатив о международном сотрудничестве на Севере, получивших название «Мурманских».

Как одному из участников их подготовки[86] хотелось бы отметить достаточно смелый характер идей, некоторые из них актуальны в регионе и по сей день. Вместе с тем, в своей речи М.С.Горбачев сделал - в угоду антиперестроечных сил - резкий выпад против НАТО: «И в тоже время здесь явственно ощущается леденящее дыхание «Полярной стратегии» Пентагона»[87].

Несмотря на успешно функционирующие здесь Совет Баренцева/Евро-арктического региона, Арктический совет и ряд иных форумов, стереотипы холодной войны, к сожалению, все еще не изжиты и их рецидивы находят отражение в различных экспертных оценках и сценариях.

Так, в докладе Национального совета по разведке (НСР) США «Глобальные тенденции до 2025 г.: преобразование мира» (2008 г.) даются следующие выводы:

- к 2025 г. завершится переход к многополярному миропорядку, роль США станет «менее доминирующей», но новые центры еще не способны принять на себя глобального управления;

---

[86] См. Смирнов А.И. Баренцев-Евроарктический регион: российско-норвежские отношения. Агентство «Бизнес-пресс», М.: 2002

[87] Главное теперь – практическое осуществление задач перестройки. Сборник материалов о поездке М.С.Горбачева в Мурманскую область. М., Политиздат. 1987. С.33

- «вакуум силы» повысит конфликтный потенциал в мире;
- ООН, ЕС, ВТО, МВФ, Всемирный Банк престанут эффективно справляться со стоящими перед ними задачами;
- **Россия может извлечь преимущества в Арктике из-за потепления, которое даст доступ к запасам газа и нефти в Сибири и на шельфе, активизирует Севморпуть**.

При всей пропагандистской заряженности и методологических неувязках доклад НСР хорошо фактурирован в стратегических интересах США. При этом очевидна озабоченность разведсообщества США поиском новой роли в полицентричном мире (в предыдущем докладе НСР от 2004 г. по проекту 2020 доминирование США в мире под сомнение не ставилось).

Контент-анализ показал, что утвержденные 18 сентября 2008 г. «Основы государственной политики Российской Федерации в Арктике на период до 2020 г. и на дальнейшую перспективу», равно как и разработанный в соответствии с Основами проект «Стратегии развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2020 года» вызвали у ряда экспертов НСР неодобрительные отзывы.

В этой связи следует отметить, что **Основы нацелены на:**

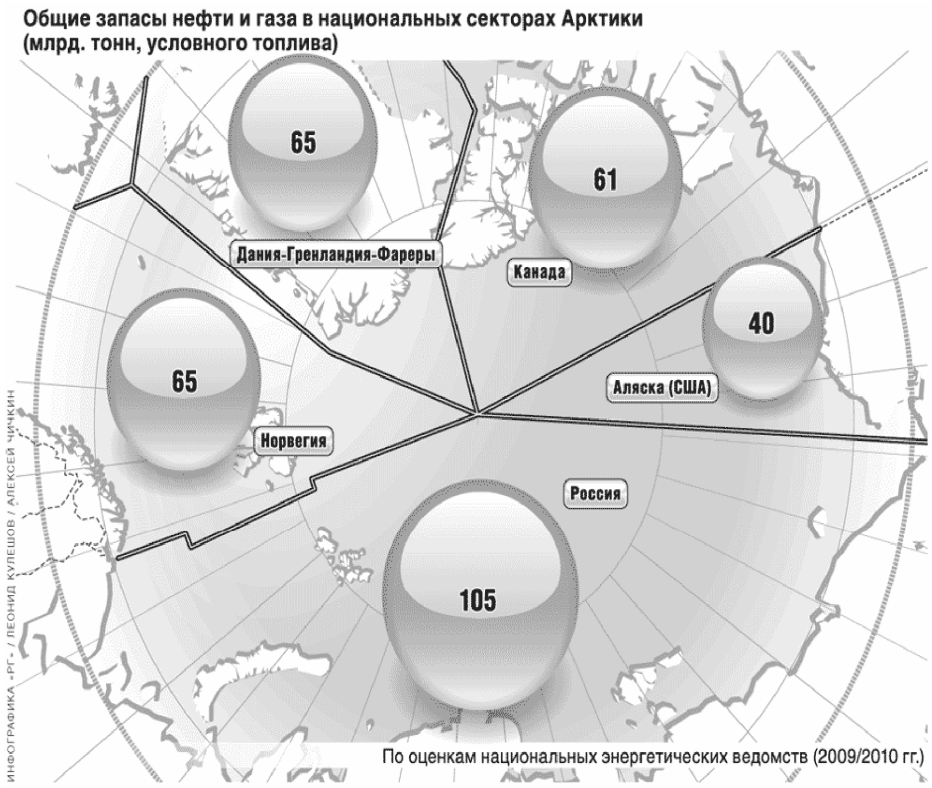
- решение внутренних задач России;
- последовательность линии в Арктике по реализации национальных интересов России (принятие документа Советом безопасности и его утверждение Президентом России подчеркивает приоритетность поставленных задач, а также гарантирует их выполнение);
- хозяйственное освоение Арктики осуществляется при сохранении уникальных арктических экосистем;
- обеспечение военной безопасности России в Арктике путем укрепления пограничных войск, береговой охраны и инфраструктуры, а также усиления контроля за обстановкой будет осуществляться лишь войсками общего назначения. **Создание каких-то «специальных арктических войск» документом не предусматривается**.

Основы подчеркивают приверженность России своим обязательствам по международным договорам и соглашениям по Арктике, в т.ч. при определении границ континентального шельфа в соответствии с Конвенцией ООН по морскому праву 1982 г. (с подготовкой геолого-геофизических, гидрографических и картографических материалов для международно-правового оформления).

С учетом того, что Арктика - это «Клондайк» минеральных, углеводородных и биоресурсов, она уже давно стала объектом кон-

куренции. За 10-15 лет в США, Японии, Южной Корее, Норвегии **созданы технологии для добычи нефти и газа на глубинах свыше 2 км. в ледовой обстановке**.

Соседи России ведут геологоразведку шельфа, определяют его границы, чтобы **закрепить права** на разработку месторождений, в первую очередь нефти и газа[88].



[88] РГ-Бизнес № 776 от 16 ноября 2010 г.

5.1.1. Кто претендует на Арктику?

В 2001 г. Россия подала заявку на расширение границ шельфа в Арктике на 1,2 млн.кв.км. (сегодня у нас 6,5 млн.кв.км. шельфа).

США, не являясь участниками Конвенции 1982 г., накануне ее рассмотрения представили целую дипломатическую ноту. В ней они оспаривали научные данные о принадлежности хребтов Ломоносова и Менделеева к континентальной окраине России, пытаясь доказать, что они являются вулканическими образованиями. Все это сыграло негативную роль - заявка была отложена до предоставления новых данных.

5.1.2. Евросоюз и Арктика

По итогам заседания Совета ЕС по внешним связям 8 декабря 2009 г., принято заявление, дающее высокую оценку докладу

«Европейский союз и Арктический регион» и завершению работы по формулированию соответствующей Стратегии ЕС к июню 2011 г. При этом Совет ЕС определил три основные цели:

1. Осуществление природоохранных мероприятий в Арктике не в ущерб коренному населению.

2. Стимулирование устойчивого использования природных ресурсов.

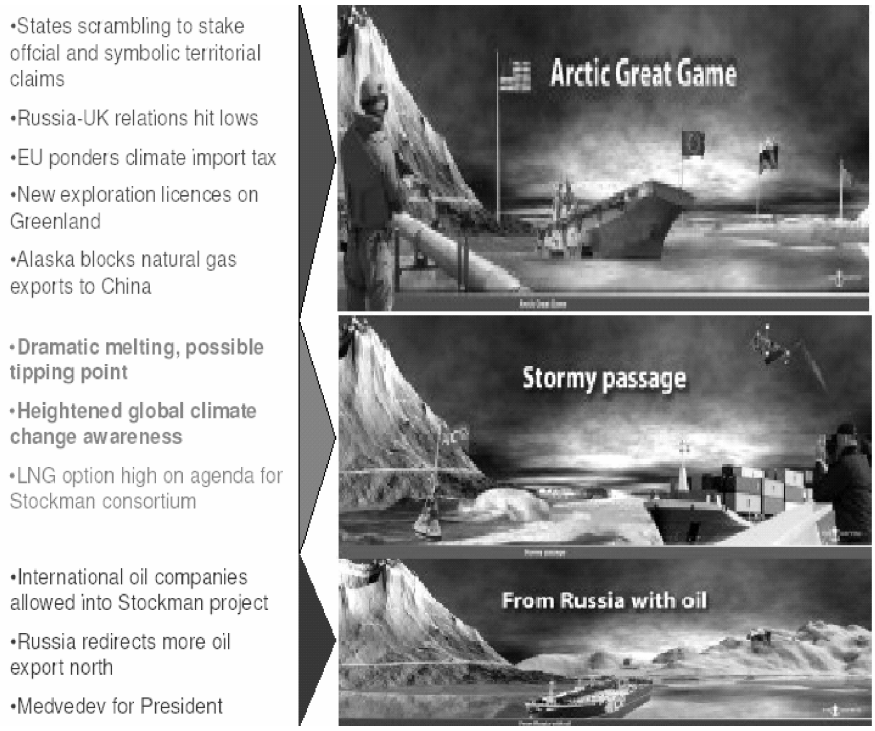
3. Оптимизация системы управления в Арктике путем реализации международных соглашений и договоренностей и задействования соответствующих механизмов.

Вывод очевиден: тема интернационализации Арктики, по всей видимости, будет активно эксплуатироваться ЕС для получения доступа и контроля над использованием ресурсов региона.

5.1.3. Сценарии развития ситуации в Арктике

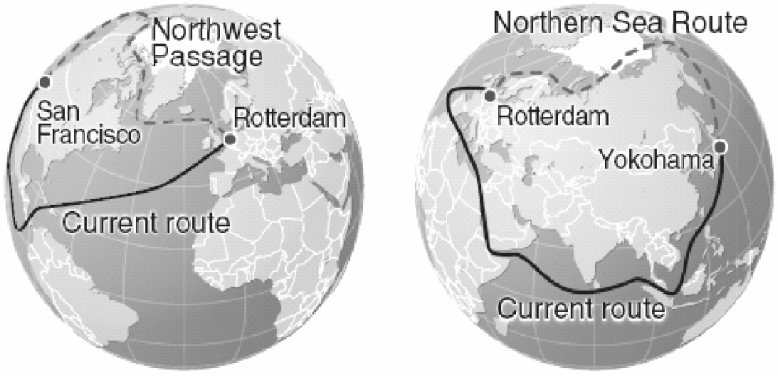
Зарубежные эксперты разрабатывают различные сценарии развития в Арктике. Наиболее интересна версия (2008 г.), которая приводится ниже. Упрощенно сценарий представлен в виде триады версий:

- конфронтационной;
- драматического потепления;
- из России с нефтью.



Отбросив конфронтационный сценарий, обращает на себя внимание влияние потепления в Арктике, которое кардинально меняет глобальную логистику и роль Севморпути в ней, т.к. появляется Северо-Западный проход.

Потепление: глобальные сдвиги в логистике



Увеличение поверхностных вод в полярных регионах обеспечит доступ к запасам нефти и газа и будет способствовать развитию судоходства по новым маршрутам с сопровождающими рисками и выгодами

5.1.4. Россия – Норвегия «Управляя Арктикой»

В совместной статье Мининдел России С.В.Лаврова и Норвегии И.Г.Стере «Управляя Арктикой»[89], («Globe and Mail», 21 сентября 2010 г.) министры не согласились с мнением ряда экспертов, что Арктика «…это регион, в котором не действует закон и который способен стать источником конфликта из-за набирающей скорость «гонки за Северный полюс».

У министров были на это веские основания, ибо 15 сентября 2010 г. в Мурманске Россия и Норвегия подписали двусторонний Договор о разграничении морских пространств и сотрудничестве в Баренцевом море и Северном Ледовитом океане. Договор устанавливает линию разграничения ранее спорного района площадью около 175000 кв.км, района потенциально богатого природными ресурсами. Обе страны условились также принять подробные договорные положения о сотрудничестве в разработке месторождений углеводородов и управлении рыбными ресурсами.

[89] http://www.mid.ru/brp_4.nsf/2fee282eb6df40e643256999005e6e8c/90fd5731ec89d9c7c32577a6004a8a82?OpenDocument

Это соглашение готовилось свыше 40 лет. В конце концов, морское право дало основу, позволившую преодолеть логику соперничества за нулевую сумму и выйти на нахождение взаимовыгодного результата.

Следует подчеркнуть, что свою роль в нахождении варианта решения сыграла Картографическая база данных ГИС «CARIS LOTS Article 76», которая была разработана в соответствии с Конвенцией ООН по морскому праву 1982 г., с учетом части IV «Континентальный шельф» (рассмотрена в 3.7.1.5.).

Министры сообща извлекли из опыта взаимодействия три урока.

Первый урок, по их мнению, состоит в том, что огромная польза, как для отдельных стран, так и для всего международного сообщества может быть получена в том случае, **если стороны будут рассматривать свои интересы в долгосрочной перспективе.** Таким примером и стала граница в Баренцевом море и Северном Ледовитом океане, ибо выигрыш, который, благодаря урегулированию вопроса теперь получит каждая из стран, значительно превзойдет то преимущество, которое одна страна в будущем могла бы получить, добиваясь сохранения большей части морского пространства.

При этом соглашение открывает возможности для взаимодействия в других областях - от научного сотрудничества до выработки стандартов в сфере безопасности мореплавания и экологии для будущего развития местных сообществ, проживающих на севере обеих стран.

Второй урок. Российско-норвежский опыт доказывает, что **Конвенция ООН по морскому праву дает основу для решения проблем, которые будут возникать по мере изменения климата в Арктике и Северного Ледовитого океана**. Это было также подчеркнуто в принятой Илулиссатской декларации 2008 года пятью приарктическими государствами, граничащими с центральной частью Северного Ледовитого океана - Канадой, Данией (Гренландией), Норвегией, Россией и США.

Третий урок состоит в том, что **ставка на диалог является решающим фактором для того, чтобы укрепить доверие между сторонами в международных отношениях.** В этом контексте одной из важных площадок является Арктический совет, в рамках которого проходят встречи представителей восьми государств Арктики на политическом и экспертном уровне, и Совет Баренцева/Евроарктического региона. Они являются важными форумами для развития диалога, укрепления доверия и интеграции новых зна-

ний в процессы проведения политики и принятия решений. Укрепление этих институтов, таким образом, является важнейшим капиталовложением.

Важность подписанного Соглашения была подчеркнута в выступлении В.В.Путина на Международном арктическом форуме в Москве 22-23 сентября 2010 г. «Арктика - территория диалога», а также на выездном заседании Морской коллегии при Правительстве России (в рамках второго международного экономического форума в г.Мурманске 30 сентября-3 октября 2010 г.).

Соглашение уже приносит результаты. В октябре 2010 г. с помощью уникального норвежского эхолота на судне «Академик Федоров» получены необходимые данные по шельфу. В 2011 г. будут проведены сейсмические работы с тем, чтобы к 2013 г. повторно направить весь пакет документов и образцов в комиссию ООН.

Актуальность данной проблемы была подчеркнута 13 декабря 2010 г. на заседании Совета Безопасности России «О состоянии и мерах по обеспечению энергетической безопасности Российской Федерации».

Главный вывод - чтобы политический климат определялся не полярным дыханием рецидивов подозрительности и страха времен холодной войны, а теплым Гольфстримом взаимовыгодного сотрудничества, в центре внимания которого, наряду с государственными интересами, прежде всего интересы рядовых северян.

5.2. Международная информационная безопасность и глобальная культура кибербезопасности

5.2.1. Информационная революция и национальная безопасность

Как уже отмечалось, планета охвачена беспрецедентной информационной революцией, которая, по мнению многих экспертов, стала локомотивом и нервом глобализации[90]. Наряду с несомненным позитивом ее феномен несет в себе принципиально новые глобальные вызовы и угрозы. Действительно, казавшиеся незыблемыми понятия меняются: по-новому воспринимаются вопросы обеспечения государственного суверенитета и национальной безо-

[90] См. Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности. М.: Парад, 2005 (www.polpred.ru)

пасности, **поскольку в условиях информационного общества границы государства становятся технологически проницаемыми**.

В силу этого в условиях глобализации значительно повысилась 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 не только России, но и всех стран.

Модернизационные императивы стали общими для всех без исключения государств. Как подчеркнул на заседании Петербургского международного экономического форума 18 июня 2010 г. Президент России Д.А.Медведев, развитие ИКТ - одно из приоритетных направлений модернизации экономики России и перевода ее на инновационное развитие. Данный фактор значительно актуализирует проблематику обеспечения международной информационной безопасности (МИБ) для национальных интересов.

5.2.2. Международная информационная безопасность как международно-правовая проблема

Проблема ограничения разработки и применения информационного оружия трансформировалась из технологической в политическую, так как, по данным ЦРУ, им занимаются свыше 120 стран мира, в то время как разработкой оружия массового поражения - около 30.

В силу этого Россия инициативно постановила вопрос об обеспечении МИБ в ООН: 23 сентября 1998 г. Генсекретарю ООН было направлено специальное Послание по проблеме МИБ Министра иностранных дел России И.С.Иванова[91]. 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.

Предварительно наша позиция по МИБ была рассмотрена и одобрена на заседании Совета Безопасности России, а затем нашла отражение в Окинавской хартии глобального информационного общества (2000 г.), Доктрине информационной безопасности (2000 г.), Стратегии развития информационного общества России (2008 г.), Стратегии национальной безопасности до 2020 г. (2009 г.), а также госпрограммы «Информационное общество (2011-2020 гг.) от 20 октября 2010 г. Проблематика МИБ как объекта исследования в 2009 г. включена Научным советом Совбеза России в число приоритетных (п.40).

В соответствии со Стратегией национальной безопасности России до 2020 года, решениями Президента Российской Федерации Д.А.Медведева **предусмотрен комплекс мер по продвижению инициативной позиции России, направленной на создание глобальной системы обеспечения МИБ**.

Важным шагом в понимании специфики проблематики МИБ стала предложенная Россией и принятая консенсусом в 1998 г. резолюция Генассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Резолюция призывала к рассмотрению существующих и потенциальных угроз в сфере информационной безопасности, определению основных понятий, оценке целесообразности разработки соответст-

[91] http://www.mid.ru/ns-dvbr.nsf/71ff2dbff09d113b43256a65002aa93b/4c86fcb9f8dc1b41c3256e320029b1ef?OpenDocument

вующих международных принципов. В принятом в 1999 г. Генассамблеей ООН обновленном проекте данной резолюции № 54/49 впервые была сформулирована «триада угроз» в сфере МИБ: применение информационных технологий в военных, террористических и преступных целях[92].

Резолюция ГА ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» постоянно получает широкую поддержку со стороны международного сообщества. Так, 28 октября 2010 г. на 65-й сессии ГА ООН Первым комитетом консенсусом был принят обновленный российский проект данной резолюции. Число соавторов нашего проекта возросло до 36 государств, в т.ч. всех наших партнеров по ОДКБ, ШОС, БРИК и других стран, в частности таких «тяжеловесов» как США, Япония, Германия и Канада.

В резолюции отмечается результативная работа Группы правительственных экспертов (ГПЭ) ООН, действовавшей под российским председательством, и подготовленный ею доклад Генсекретаря ООН, посвященный актуальным исследованиям угроз международной безопасности в информационной сфере. В докладе нашли отражение все ключевые положения позиции России по проблематике обеспечения МИБ.

Принятая резолюция подтверждает решение о воссоздании в 2012 г. ГПЭ с тем, чтобы продолжить исследование существующих и потенциальных угроз в сфере информационной безопасности и выработку возможных совместных мер по их устранению, а также концепций, направленных на укрепление безопасности глобальных ИТКС.

Таким образом, цель усилий России на мировой арене - не допустить очередного витка гонки вооружений, пресечь использование ИКТ для решения задач, противоречащих интересам обеспечения международного мира и стабильности, суверенитета и безопасности государств.

Особую актуальность данной проблематике придает тот факт, что ИКТ 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.

Тема обеспечения МИБ с подачи России заняла прочное место в повестке дня целого ряда авторитетных международных форумов,

[92] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/777/15/PDF/N9977715.pdf?OpenElement

включая ОБСЕ (Форум по сотрудничеству в области безопасности), ШОС, ОДКБ, Совет Европы, «Группу восьми», АСЕАН (Региональный форум по безопасности), Международный союз электросвязи, Форум по управлению Интернетом, созданный под эгидой ООН.

Наиболее значимым для России результатом стало подписание 16 июня 2009 г. в Екатеринбурге в ходе саммита ШОС Соглашения между правительствами государств-членов ШОС о сотрудничестве в области обеспечения МИБ[93]. Соглашение было разработано на основе проекта, сформулированного и предложенного российской стороной, в рамках действующей под председательством России Группы экспертов государств-членов ШОС по МИБ.

Целью Соглашения является создание политико-правовых и организационных основ дальнейшего углубления доверия и развития взаимодействия Сторон и национальных компетентных органов в области МИБ.

Соглашение определяет наличие и существо конкретных угроз в области МИБ, а также основные направления, принципы, формы и механизмы сотрудничества сторон в этой сфере. Соглашение открыто для присоединения других государств, что позволит расширить географические рамки его действия. Важно, что Соглашение стало первым в международной практике договорным актом, направленным на ограничение всего комплекса угроз МИБ.

Информационная безопасность, давно вышедшая за рамки борьбы с известными киберпреступлениями, определенными Интерполом (хакинг[94], крекинг[95] 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 ИКТ, игнорируя действующие международно-правовые дефиниции их статуса.

В качестве универсального договорного документа в сфере МИБ западные страны, прежде всего США, позиционируют Конвенцию о киберпреступности Совета Европы 2001 г.

---

[93] http://sco2009.ru/docs/documents/

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

[95] Крекинг – криминальный хакинг (киберпреступление)

Однако использование данной Конвенции представляется для России неприемлемым в первую очередь по причине ее ограничительного характера в отношении сферы применения, т.к. военно-политический аспект проблематики МИБ данным документом никак не рассматривается. Конвенция также не учитывает уровень и особенности развития ИКТ в странах, находящихся за пределами европейского региона. Данная Конвенция сосредоточена прежде всего на борьбе с враждебными информационными атаками против компьютерных систем и, следовательно, не направлена напрямую на укрепление общей информационной безопасности и не позволяет международному сообществу адекватно реагировать на новые вызовы и угрозы в области МИБ, а также вступает в явное противоречие с нормами международного права.

Так, согласно пункту «b» статьи 32, сторона Конвенции может иметь через компьютерную систему на своей территории доступ к компьютерным данным, хранящимся в другом государстве, тоже являющемся стороной Конвенции, или получить их без его согласия, если эта сторона заручится законным и добровольным согласием лица, имеющего законные полномочия раскрывать упомянутые данные указанной стороне через такую компьютерную систему.

Поскольку Конвенция не содержит определения понятий «обыск», «выемка», «доступ», «лицо, имеющее законные полномочия раскрывать данные», положения пункта «b» статьи 32 на практике могут толковаться как предоставляющие право производства трансграничного обыска в компьютерных сетях без согласия заинтересованной стороны.

Более того, применение ряда положений этого документа (в частности, пункта «b» статьи 32) может нанести ущерб суверенитету и национальной безопасности государств-участников. Фактически формулировка упомянутого пункта означает, что иностранные правоохранительные органы (а, значит, и спецслужбы) могут работать напрямую с гражданами государств - участников Конвенции на их территории с целью получения необходимой информации. Это предполагается делать не только без согласия, но даже без уведомления государства их гражданства. Очевидно, что здесь имеет место нарушение принципа суверенитета государств, который предусматривает осуществление своей юрисдикции в отношении находящихся на их территории физических и юридических лиц, а также прав и свобод человека, в т.ч. права на юридическую защиту от возможных злоупотреблений правоохранительных органов и спецслужб иностранных государств. Тем самым не только легализуется прямой выход на физических и юридических лиц правоохра-

нительным органам и спецслужбам иностранных государств, но и создается нежелательный прецедент. Следовательно, говорить о равноправном партнерском сотрудничестве в борьбе с киберпреступностью в таких условиях не представляется возможным.

Стремительные темпы развития и внедрения новых ИКТ, формирование глобального киберпространства порождают как новые виды преступлений, так и новые методы противодействия им. Конвенция, разработанная до 2001 г., этих новых моментов не учитывает. При этом статья 42 Конвенции исключает возможность внесения в нее оговорок и изменений, а, следовательно, и модернизацию этого объективно устаревшего документа.

Необходимо отметить также, что Конвенция, изначально разработанная в интересах государств-членов Совета Европы, не учитывает уровня и особенностей развития ИКТ в странах других регионов. Кроме того, она может негативно сказаться на процессе развития национальных законодательств и понимании принципов международной информационной безопасности в тех странах, в которых к изучению этой проблематики обратились лишь недавно.

Современное российское законодательство в данной области не только охватывает весь спектр положений Конвенции, но по многим позициям включает более универсальные и рассчитанные на перспективу нормы. Таким образом, для России участие в Конвенции было бы шагом назад.

Учитывая вышеизложенное, российская сторона считает предложения о присоединении к Конвенции неприемлемыми и не рассматривает его как базовый или как самодостаточный документ в области борьбы с киберпреступностью, а тем более - в области МИБ.

С учетом этих факторов многие государства разделяют предлагаемую Россией идею разработки универсальной международной конвенции о борьбе с преступностью в сфере ИКТ (киберпреступностью). Такая универсальная конвенция призвана разрешить целый ряд фундаментальных вопросов, не нашедших адекватного отражения в Конвенции Совета Европы, а именно: обеспечить национальный суверенитет государств-участников, соблюдение прав их граждан и одновременно гарантировать эффективность международного сотрудничества по предупреждению и пресечению преступлений в сфере ИКТ. Предполагается, что новая конвенция покроет все возможные составы преступлений, а также будет предусмотрена возможность адаптации к новым видам преступной деятельности в информационном пространстве.

На 12-ом Конгрессе ООН по предупреждению преступности и уголовному правосудию (апрель 2010 г., Бразилия), выдвинутая Россией идея универсальной конвенции встретила жесткую оппозицию со стороны США и ряда стран-членов ЕС. Только угроза срыва итогового документа Конгресса - Сальвадорской декларации - позволила включить в него рекомендацию в адрес Комиссии ООН по предупреждению преступности и уголовному правосудию учредить межправительственную группу по проблематике киберпреступности с мандатом для разработки такой конвенции.

Сторонники универсальной конвенции ООН, включая Группу 77 и партнеров по БРИК, ожидают от России инициатив в разработке такого документа с учетом наших политических, интеллектуальных, технических и иных ресурсов в области борьбы с преступностью в сфере ИКТ.

Работу над таким документом можно было бы логически вписать в контекст идей России по выстраиванию в рамках ООН глобальной системы обеспечения МИБ, в данном случае в уголовно-правовой сфере.

Системное изучение проблематики МИБ подтверждает, что способы и особенности использования ИКТ, в т.ч. латентные, 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 наряду с информационным оружием включает в себя и информационно-психологическую безопасность.

5.2.3. Прогнозы по продвижению МИБ

Для закрепления и развития достигнутых результатов и дальнейшего продвижения российской инициативы в области формирования системы МИБ в качестве рекомендаций по подходам России в области формирования системы МИБ представляются оправданными следующие прогнозы:

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

- учитывая специфику ИКТ, способы и особенности их возможного использования во враждебных и неправомерных целях, в триаде угроз информационной безопасности - военно-политиче-

ского, криминального и террористического характера - приоритетное значение будет иметь военно-политическая составляющая;

- продолжится противодействие предложениям использовать в качестве универсального договорного документа в сфере МИБ Конвенцию Совета Европы о киберпреступности (Будапештская конвенция) 2001 г. и, соответственно, продвижение российской идеи разработки универсальной международной конвенции о борьбе с преступностью в сфере ИКТ (киберпреступностью);

- в контексте проблематики МИБ вопросы использования Интернета будут ориентироваться на решения Всемирной встречи на высшем уровне по вопросам информационного общества (2003-2005 гг.), в т.ч. по интернационализации управления Интернетом, обеспечения равноправного участия государств в его управлении, реализации суверенного права государств на самостоятельное управление Интернетом на национальном уровне, повышения роли Международного союза электросвязи в управлении Интернетом (на международной основе), гарантирования непрерывности, безопасности и стабильности его функционирования;

- центром проведения политики России в области МИБ останется ООН, в т.ч. в формировании и работе созываемой в 2012 году в соответствии с решением Генассамблеи ООН Группы правительственных экспертов ООН;

- активизируется работа по формированию системы информационной безопасности государств-членов ОДКБ;

- в международном общении будет активнее применяться терминология по проблематике МИБ, разработанная в России и согласованная в рамках ШОС.

5.2.4. Проблема глобальной культуры кибербезопасности

Проблематика МИБ тесно переплетается с резолюциями ООН о создании глобальной культуры кибербезопасности.

Так, ГА ООН 17 марта 2010 г. приняла резолюцию (по докладу Второго комитета A/64/422/Add.3) «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур». Данная резолюция стала развитием ранее принятых резолюций (55/63 от 4 декабря 2000 года и 56/121 от 19 декабря 2001 года о борьбе с преступным использованием информационных технологий, 57/239 от 20 декабря 2002 года о создании глобальной культуры кибербезопасности в 58/199 от 23 декабря 2003 года о создании глобальной культуры ки-

бербезопасности и защите важнейших информационных инфраструктур).

Признавая растущий вклад ИКТ во все сферы социума, ООН призвала правительства, деловые круги, организации и индивидуальных владельцев и пользователей ИКТ к ответственности за обеспечение безопасности и принятие надлежащих мер для ее укрепления.

Особое место в резолюции уделено важности мандата Форума по вопросам управления Интернетом: «все правительства должны иметь равные задачи и обязанности в сфере управления Интернетом на международной основе и обеспечения стабильности, безопасности и непрерывности Интернета».

В резолюции также отмечено, что угрозы надежному функционированию важнейших инфраструктур ИКТ и целостности информации, передаваемой по этим сетям, приобретают все более изощренный и серьезный характер, отрицательно сказываясь на уровне семейного, национального и международного благополучия.

В силу этого в резолюции подчеркнуто, что национальные усилия должны подкрепляться обменом информацией и взаимодействием на международном уровне, с тем, чтобы можно было эффективно противостоять новым угрозам, приобретающим все более транснациональный характер.

В этом контексте подготовленный Международным союзом электросвязи в 2009 г. доклад об обеспечении защищенности ИКТ и передовой практике в области формирования культуры кибербезопасности основное внимание уделяет всеобъемлющему национальному подходу к кибербезопасности, не нарушающему свободы слова, свободы передачи информации и надлежащих правовых процедур.

С учетом вышеизложенного в резолюции ООН предлагается государствам-членам использовать инструмент добровольной самооценки национальных усилий по защите важнейших информационных инфраструктур, призванный помочь им выявить области, в которых требуется принятие дополнительных мер, в целях повышения глобальной культуры кибербезопасности. Кроме того, рекомендовано государствам-членам и соответствующим региональным и международным организациям, разработавшим стратегии действий в области кибербезопасности и защиты важнейших информационных инфраструктур, поделиться сведениями о передовой практике и мерах, которые могли бы помочь другим странам по обеспечению кибербезопасности.

Как уже отмечалось выше, Россия инициативно и ответственно относится к данной проблематике. Одним из важных документов последнего времени (май 2009 г.) стала Стратегия национальной безопасности Российской Федерации до 2020 года. Ее пункт 109 гласит, что «угрозы информационной безопасности в ходе реализации настоящей Стратегии предотвращаются за счет совершенствования безопасности функционирования ИКТ систем критически важных объектов инфраструктуры и объектов повышенной опасности в России, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности».

В этом контексте в России уточнены роль и обязанности заинтересованных сторон, стратегические процессы и участие, сотрудничество между государственным и частным секторами, деятельность в связи с инцидентами и восстановление после сбоев, а также правовые нормы и формирование глобальной культуры кибербезопасности.

Заметный вклад в столь важный процесс вносят институты гражданского общества, в т.ч. национальный форум по информационной безопасности «ИНФОФОРУМ».

В России разработано необходимое законодательство для расследования киберпреступлений и преследования лиц, виновных в их совершении, с учетом существующих механизмов, в т.ч. резолюций 55/63 и 56/121 Генеральной Ассамблеи о борьбе с преступным использованием ИКТ.

5.2.5. Интернет 2025 – прогноз сценариев развития

С учетом стремительного процесса интернетизации планеты эксперты Cisco и Monitor Group прогнозируют в отчете «The Evolving Internet»[96] («Растущий интернет»), что в течение ближайших 15 лет Интернет будет развиваться по одному из следующих сценариев.

Первый сценарий называется Fluid frontiers («Жидкие границы»). Он описывает мир, в котором Интернет будет распространен еще больше, а его роль будет являться критически важной. В этом случае ожидается дальнейший рост мирового Интернет-предпринимательства вместе с ужесточением

[96] http://newsroom.cisco.com/dlls/2010/prod_082510b.html

конкуренции в этой сфере, которая приведет к появлению огромного числа новых технологий.

Второй сценарий, Insecure growth («Небезопасное развитие»), описывает возможность того, что пользователи и организации столкнутся с ухудшением безопасности, страдая от бесчисленного количества кибератак. В этом случае аналитики ожидают, что появятся более безопасные альтернативы Интернету, однако они будут платными и дорогостоящими.

Третий вариант Short of the promise («Не оправдать ожиданий») предполагает, что экономический застой во многих странах отразится и на развитии Интернета. В этом случае рецессия и протекционистская политика сильно замедлят рост сети и появление инноваций.

Четвертый вариант предполагает развитие событий, в рамках которого Интернет станет жертвой собственного успеха Bursting at the seams («Разрываясь по швам»). В этом случае спрос на различные веб-сервисы окажется так велик, что ИКТ не смогут справиться с объемами трафика.

Авторы предсказывают, что система управления Интернетом в будущем не сильно изменится, хотя тарифов для оплаты станет гораздо больше. QWERTY-клавиатура перестанет быть основным устройством управления, а пользователи, знакомые с Интернетом с детства, будут относиться к этой среде совсем иначе, чем нынешние. Прогнозируется, что основной рост в течение следующих 15 лет придется на развивающиеся страны, где доступ к нему пока невелик.

Все вышеизложенные сценарии развития Интернета еще раз подчеркивают актуальность обеспечения и МИБ, и культуры кибербезопасности, за продвижение которых последовательно выступает Россия.

5.3. Мутация терроризма как вида асимметричной войны

Данной тематике посвящено огромное количество научных и специальных исследований. Терроризм может иметь несколько разновидностей в зависимости от того, какое именно меньшинство является субъектом теракта. Выделяют следующие основные категории терроризма:

- идеологический;
- этнический;
- религиозный;

- криминальный;
- индивидуальный;

Для лучшего понимания эволюции терроризма как вида асимметричной войны обратимся к наиболее известным работам за последние 100 лет.

5.3.1. Анализ симметричных войн

Еще в годы первой мировой войны англичанин **Ф.Ланчестер** (F.Lanchester) разработал ряд уравнений для расчета баланса сил армий в классической симметричной войне, в которой две иерархически организованные армии сражаются до победы. Ф.Ланчестер доказал, что сила армии, которая использует оружие, поражающее за один раз много целей, пропорциональна квадрату ее огневой мощи. Сосредоточение огневой мощи, разделение сил противника, а также устранение лидеров противника или лишение подразделений врага управления остаются ключевыми правилами тактики.

Другие подходы были использованы для изучения войн в 1948 г. английским физиком и пацифистом **Л.Ф.Ричардсоном** (L.F.Richardson). Исследуя потери от всех войн в период между 1815 и 1945 гг., он разделил конфликты по числу погибших. Выявился определенный тренд: мелкие стычки с несколькими жертвами стали обычным явлением, а крупные войны с многочисленными жертвами - редкими.

Данная экспоненциальная (возрастающая) кривая контрастирует с кривой нормального распределения в виде «колокола», когда события среднего масштаба наиболее часты, а очень значительные и очень незначительные события редки. Аналогичная закономерность была выявлена и в других сложных системах с большим количеством смертей. Так, малые землетрясения происходят чаще, чем средние, а средние чаще, чем крупные, и т.д.

5.3.2. Исследование асимметричных конфликтов

Анализируя статистику смертей от терактов с 1968 г., ученый из института Санта Фе в Нью-Мексико **А.Клосе** (A.Clauset) обнаружил, что **терроризм еще больше соответствует экспоненциальному закону, чем обычные войны**. Более того, точная форма кривой варьируется в зависимости от региона. Теракты в промышленно

развитых странах занимают место в начале графика, т.е. их вероятность ниже, но и масштабы больше. В то же время теракты в развивающихся странах более вероятны, но они менее крупные. А.Клосе объясняет это тем, что в развивающихся странах легче достать оружие, а в промышленно развитой стране есть множество уязвимых для терактов объектов инфраструктуры.

Н.Джонсон (N.Johnson) и его коллеги из университета в Майами сравнили статистику смертности во время ряда боестолкновений в симметричных конфликтах и в конфликтах против различных «повстанцев», в которых регулярная армия берет на себя борьбу с террористами или борцами за свободу. **Для ассиметричных конфликтов экспоненциальный рост особенно очевиден: каждый из них имел экспоненциальный рост с градиентом, близким к 2,5.**

Можно предположить, что проблемы асимметричных войн можно решить сокращением мелких конфликтов. Однако это не так просто. Крупные конфликты с большим количеством жертв все равно будут подчиняться экспоненциальному закону и при изъятии мелких стычек. В крупных столкновениях может погибнуть больше людей, чем во множестве незначительных инцидентов. Так, по мнению **Б.Тивнена** (B.Tivnan) из MITRE Corporation, в Афганистане ресурсы должны направляться не только на борьбу с мелкими нападениями повстанцев. Это изменит риски и быстро напомнит нам, что крупные события тоже имеют не нулевую вероятность. Если же бороться только с нападениями среднего масштаба, значительно искажается картина обстановки.

Н.Джонсон представил свою модель поведения террористических групп на конференции по «оперативной адаптации» к изменяющимся условиям войны, которую организовали ВМС США в университете Эдинбурга (Великобритания). Модель отражает две характерные особенности террористических групп: их динамичное объединение и распад, а также зависимость от связи на больших расстояниях и наличия СМИ. Особую роль играют СМИ, которые используются террористами как трибуна для обращения к общественности, - поделился своим мнением **Л.-Э.Седерман** (Lars-Erik Cederman) из Международного центра исследования конфликтов в Швейцарском федеральном технологическом институте. Он предостерег от чрезмерного упрощения: **предсказать теракт, или развитие войны, как и других сложных систем, крайне непросто**[97]**.**

[97] http://www.cnews.ru/news/line/index.shtml?2010/08/04/403707

Тем не менее, математическая модель демонстрирует уязвимые места в сети террористической организации, например, уже упомянутые коммуникации и связь со СМИ. Также данный алгоритм, несомненно, будет полезным в борьбе с оргпреступностью и наркомафией.

5.3.3. Ведение войны асимметричными методами

Террористические удары 11 сентября 2001 г. по высотным зданиям в Нью-Йорке и по Пентагону в Вашингтоне зафиксировали начало новых в военном искусстве асимметричных войн. Они ведутся не вооруженными силами и не оружием в привычном его понимании.

Таким образом, имел место не только теракт стратегического масштаба, а фактически совершенно новый тип асимметричной войны.

Эта война отличается от войн всех предыдущих поколений своей тактикой:

- нанесено несколько сосредоточенных по времени и месту невоенных ударов,
- получен внезапный ошеломляющий результат с неприемлемым для жертвы ущербом;
- отсутствовали политические требования;
- применены и (применяются) неожиданные средства и формы насилия.

В данном случае вместо политических целей асимметричной войны явно просматривалась ненависть к политическому режиму США и к их лидерам за многие годы.

Но кто запланировал и так искусно осуществил этот акт?

Возможно, таким образом реализована накопленная злоба лидеров мировой наркомафии, с которой достаточно успешно ведут длительную борьбу США. Наркобизнес вполне реально мог стать финансовой базой этой войны. А, может быть, здесь повязаны стратегические планы нефтяных магнатов, которые заинтересованы в уменьшении конкуренции на нефтяных рынках и хотя бы в течение даже короткого времени заработать сверхприбыли. Не случайно обнаруженные, 11 сентября 2001 г., важные улики, связанные с этими терактами, были явно «направлены» против некоторых стран-экспортеров нефти.

Непровозглашение политических целей этой асимметричной войны, скрытность тех, кто взял на себя ответственность за ее про-

ведение, подтолкнули США к банальному выбору виновника: Усамы бен Ладена и укрывающих его в Афганистане талибов.

Вызывает удивление и то, что теракты «прозевали» спецслужбы США. Очевидно, что асимметричная война будет идти по правилам, навязанным международным терроризмом. Логично ожидать новых, совершенно невоенных средств и форм проведения агрессии.

В этом контексте непонятно, почему США так долго (21 день) готовились к ответным действиям, но выбрали алгоритм упрощенного варианта решения борьбы с международным терроризмом. Самоочевидно, что США просто растерялись и не знали как действовать. Далее откладывать ответный удар было просто нельзя, ибо американский налогоплательщик мог расценить это как слабость.

Что касается новых асимметричных форм насилия в теракте, то они свидетельствуют о серьезной предварительной их разработке. Ядерное оружие и его компоненты при всей «привлекательности» и масштабности возможного воздействия остаются пока недоступными для террористических группировок. В силу этого они и разработали совершенно новые формы ведения асимметричной войны и сумели отладить весь механизм подготовки и реализации этих форм, выбрав в качестве объекта удара важнейшие национальные символы США.

Результаты, на которые рассчитывал международный терроризм в этой асимметричной войне, в основном достигнуты. Эффект от теракта был ошеломляющим, а людские потери просто огромны и составляют примерно половину тех, которые официально обнародовал СССР после 10 лет военных действий в Афганистане.

США привыкли жить беспечно и не предполагали, что они могут стать объектом поражения, тем более таким неожиданным способом. Все усилия своей дипломатии направляли исключительно на парирование любых симметричных ядерных возможностей стран, отнесенных к противникам по нанесению ими бесконтактным способом неприемлемого ущерба им. США для обеспечения ядерной безопасности пошли на серьезные сокращения стратегических ядерных вооружений и на ДНВ-3.

Однако асимметричная война застала врасплох руководство страны. В первые часы после асимметричного удара президент Буш был вынужден прятаться от собственного народа и СМИ, что не осталось незамеченным. Война была разработана и осуществлена таким образом, что все мировые СМИ в прямой трансляции демонстрировали успехи терроризма.

Очевидно, что для противоборства с терроризмом в асимметричных войнах в некоторых странах потребуется в короткие сроки создать гражданский вид вооруженных сил - силы и средства гражданской защиты государства от любых возможных террористических актов, а заодно и чрезвычайных ситуаций природного и искусственного происхождения. Этот «вид» вооруженных сил должен иметь: надежную автоматизированную систему управления, свою разветвленную в стране и за рубежом специальную финансовую разведку, контртеррористические силы и средства, силы и средства спасения людей и материальных ценностей.

Только недальновидные «специалисты» продолжают заявлять, что никакие проблемы и катаклизмы не повлияют на ее создание. Нельзя исключить, что это все может быть пересмотрено. Когда все, касающееся «гражданского вида» вооруженных сил, будет рассчитано, а тем более создано и реализовано, то может оказаться, что ПРО действительно не нужна. При этом стоимость гражданской обороны страны может быть настолько большой, что на все остальные проекты может не оказаться финансовых средств. В силу этого США и другие страны будут вынуждены пересмотреть свои политические приоритеты и отношение к целому ряду мировых проблем.

5.3.4. Угроза ядерного терроризма

Под ядерным терроризмом понимается совокупность намерений и действий отдельных лиц либо группировок по созданию либо приобретению ядерного взрывного устройства (ЯВУ) с последующим его применением или угрозой применения для достижения декларируемых ими политических, социальных и иных целей.

Из определения вытекает следствие: государство при реализации этих целей выводится за скобки, оно, в лучшем для террористов случае, их старается не замечать, а в худшем - преследует их. **Вопрос о ядерном терроризме, когда государство само начинает играть роль террориста, также сегодня крайне актуален**.

Главное, без чего ЯВУ не создать, - расщепляющийся материал, которых два: уран-235 и плутоний-239, оба - оружейной чистоты (>90% и >94% соответственно).

Из этого вытекают следующие три следствия:

- наработка необходимых для создания ЯВУ количеств расщепляющегося материала силами ядерных террористов с «нуля» или даже с использованием промежуточных технологических продуктов нереальна;

- сообщения о кражах и пропажах естественного или слабообогащенного урана, радиоизотопный продукции (радиостронция, радиоцезия, радиокобальта и др.) относится к проблеме радиационного терроризма, а не ядерного;
- ядерная энергетика как таковая, за исключением захвата, интереса для ядерных террористов не представляет. Из низкообогащенного (до 5% урана-235) ядерного топлива создать ЯВУ невозможно, а из реакторного плутония, содержащегося в облученном топливе, возможно лишь в умозрительном плане.

Принципиально важную роль в пресечении этой возможности играет постановка объекта под международный контроль и инспекции МАГАТЭ.

Рассмотрим ситуацию, когда злоумышленники получат материалы для изготовления примитивного ЯВУ.

Главные проблемы поджидают террористов на этапе конструирования ЯВУ. Принцип действия ЯВУ общеизвестен. Это обстоятельство часто используется в качестве главного обоснования реальности угрозы ядерного терроризма. Но именно принцип, а не детали его конструкций.

Закрытость технологий создания ЯВУ является сегодня одним из главных препятствий, стоящих перед ядерными террористами. В силу этого экспертам по «ядерным» темам не следует переступать ту грань, за которой образовательный материал может превратиться в пособие для террористов.

5.3.5. «Цифровой джихад» и борьба с ним

Информационный терроризм - это форма негативного воздействия на личность, общество и государство всеми видами информации. Его цель - ослабление и расшатывание конституционного строя. Он может осуществляться разнообразными силами и средствами - от агентуры иностранных спецслужб до внутренних и зарубежных СМИ.

«Цифровой джихад» в сфере использования информационных систем (по американской терминологии - «кибертерроризм») - это использование информационного оружия против информсистем критически важных объектов противника.

5.3.6. ООН против терроризма

В 90-х гг. Совет Безопасности ООН принял ряд санкций против государств, которые подозревались в связях с тергуппировками: Ливия (1992 год), Судан (1996 год) и Афганистан (1999 год - движение «Талибан», 2000 год - организация «Аль-Каида»). Резолюцией 1269 (1999) Совет Безопасности призвал страны к сотрудничеству с целью предотвращения всех терактов. Эта резолюция стала началом интенсификации контртеррористической деятельности Совета после 11 сентября 2001 г.

До терактов в США 11 сентября 2001 г. Совет Безопасности создал влиятельный контртеррористический орган: Комитет 1267. Его задачей стал контроль выполнения санкций против движения «Талибан» (а с 2000 г. - «Аль-Каиды»). По просьбе Совета Безопасности, для поддержки работы Комитета, Генеральный секретарь ООН создал Группу по аналитической поддержке и наблюдению за санкциями. В состав Группы вошли эксперты по борьбе с терроризмом и смежным юридическим вопросам, по эмбарго на поставку оружия, запретам на передвижение и по финансированию терроризма.

После 11 сентября 2001 г., Совет Безопасности резолюцией 1373 (2001) учредил Контртеррористический комитет в составе всех членов Совета Безопасности. Государства-члены были обязаны регулярно докладывать Контртеррористическому комитету о принятых ими мерах по выполнению резолюции 1373.

Для оказания помощи Контртеррористическому комитету, Советом Безопасности в 2004 г. была принята резолюция 1535, учреждающая Исполнительный директорат Контртеррористического комитета (ИДКТК).

Своей резолюцией 1540 (2004) Совет Безопасности учредил новый орган, занимающийся вопросами борьбы с терроризмом, который также состоит из всех членов Совета. Комитет следит за выполнением государствами-членами положений резолюции 1540, призывающей предотвратить доступ к ОМУ негосударственными лицами (включая террористические группировки).

В 2004 г. Совет также принял резолюцию 1566, которая призвала государства-члены принять меры против групп и организаций, вовлеченных в террористическую деятельность, на которую не распространяется действие резолюции 1267. Резолюция 1566 учредила Рабочую группу для выработки рекомендаций относительно мер, которые будут применяться к отдельным лицам и группам, а

также для создания компенсационного фонда для жертв терроризма.

В рамках Всемирного саммита 2005 г. Совет Безопасности провел встречу на высоком уровне и принял резолюцию 1624, которая осудила любые теракты независимо от их мотивов и побуждений.

8 сентября 2006 г. была принята **Глобальная контртеррористическая стратегия ООН**, которая является уникальным глобальным документом, укрепляющим национальные, региональные и международные усилия по борьбе с терроризмом.

После проведения Генассамблеей второго обзора осуществления Глобальной контртеррористической стратегии ООН (A/RES/60/228) и принятия в связи с этим резолюции 64/297 Генассамблеи, Совет Безопасности провел 27 сентября 2010 г. открытые прения по вопросу об угрозах международному миру и безопасности, создаваемых терактами.

В заявлении Председателя, сделанном им после этого заседания (S/PRST/2010/19), Совет отметил, что создаваемая терроризмом угроза стала более рассредоточенной в различных регионах мира.

5.3.6.1. Особенности позиции России

Мероприятия 2010 г. в ООН прошли в условиях неослабевающей террористической угрозы, на фоне терактов во многих странах мира, которые не обошли и Россию. Так, в связи с терактом во Владикавказе Совет Безопасности ООН сделал специальное заявление.

В этом контексте необходимо отметить следующие тренды (взгляд из России):

1. Усиливается связь международного терроризма с трансграничной организованной преступностью, особенно наркопреступностью, а также с пиратством, торговлей людьми и оружием. Так, пираты у берегов Сомали делят деньги с террористическими группировками, такими, как, например, «Аль-Шабаб». Ярким примером опасной смычки «терроризм-наркопреступность» является и ситуация в Афганистане, где террористическая активность и наркопреступность активно подпитывают друг друга.

2. Сохраняют актуальность вопросы устранения пробелов международно-правовой базы антитеррора и борьбы с другими связанными с терроризмом новыми вызовами и угрозами. В этой связи следует обеспечить исполнение принципа «либо выдай, либо суди», закрыть различные правовые лазейки и «тихие гавани» для террористов, в том числе прикрывающихся статусом беженца. Россия

предлагает разработать универсальную конвенцию по вопросам выдачи и взаимной правовой помощи, в которой был бы и антитеррористический компонент. Еще одним элементом совершенствования договорной базы могла бы стать разработка международной конвенции по борьбе с киберпреступностью. Важно не допускать использования Интернета в террористических целях при соблюдении принципа верховенства закона, свободы слова и права на частную жизнь.

3. Продолжать линию на подключение к решению задач противодействия терроризму потенциала гражданского общества, СМИ, делового мира. В русле выдвинутой Россией инициативы государственно-частного антитеррористического партнерства реализуются соответствующие практические мероприятия, программы и проекты, как в нашей стране, так и во многих других государствах.

Россия всегда выступает за комплексный подход в противодействии терроризму, за междисциплинарный подход, содействует целевой группе секретариата ООН по имплементации глобальной контртеррористической стратегии, объединившей более 30 структур, фондов, программ и подразделений ООН, а также Интерполу. У каждой из них свой профиль, однако каждая вносит свою «добавленную стоимость» в антитеррористический потенциал ООН.

Резюмируя, следует подчеркнуть, что в ответ на энергичные меры противодействия терроризм мутирует, вербует новых сторонников, в том числе террористов-смертников, изыскивает новые пути получения финансовых средств.

5.3.7. Схемы отмывания денег и финансирования терроризма

Авторы «Справочного руководства» по борьбе с отмыванием доходов (БОД) и борьбе с финансированием терроризма» (БФТ), изданного Всемирным Банком в 2005 г., констатируют, что преступники охотно используют страны со слабой системой для БОД и БФТ, неэффективной или коррумпированной правовой инфраструктурой. При этом все этапы (размещения, дробления и интеграции - см.схему) могут проводиться в разных странах (зачастую и не знающих о том, что стали объектом преступления).

Источник: «Справочное руководство по БОД и БФТ. Всемирный Банк, 2005 г.»

В случае с отмыванием источники средств могут быть только криминальными, в случае с финансированием терроризма - как криминальными, так и легитимными (см. журнал «Микро-finance+»). К числу таких легитимных источников могут относиться пожертвования, денежные или имущественные дары, предоставляемые таким организациям, как фонды или благотворительные учреждения.

Для принятия действенных мер по БФТ (как правило, они автоматически включают и меры по БОД) страны-участницы международных альянсов, групп и организаций постоянно расширяют свою правовую базу, распространяя ее действие и на некоммерческие организации (особенно на благотворительные учреждения), чтобы предотвратить возможность прямого или косвенного их использования.

В силу глобальности проблемы многие страны вынуждены решать ее через привлечение к сотрудничеству международных организаций: ООН, Всемирный Банк, МВФ, FATF, Базельский комитет по банковскому надзору, Международную ассоциацию страховых надзоров, Международную организацию комиссий по ценным бумагам, Группу подразделений финансовой разведки «Эгмонт», региональные органы и компетентные группы и т.д.

МВФ оценивает общий объем денежных средств, отмываемых во всем мире в 2-5% от мирового валового национального продукта, т.е. 1,0-1,5 трлн.долл. Для легализации и отмывания таких сумм нужно время, деньги (затраты на отмывание), выбор вариантов, исполнители. Суммы дробятся, расходятся по слоям, вовлекая в процесс отмывания все новых и новых людей. Апробируются, не считаясь с затратами, новые схемы, при которых отмывочные деньги вливаются в общий финансовый поток законного бизнеса, меняя свой статус (отмываясь) без обналичивания.

Международный опыт говорит, что если преступникам удается в течение суток 7 раз перегнать деньги по разным странам, то выявить и доказать их криминальную природу практически не возможно. Для запутывания ситуации достаточно и двух шагов, если они сделаны в странах, где антиотмывочные законы либеральны или их нет вообще.

Успешно противодействуют «мойщикам» те финансовые организации, у которых деятельность прозрачна, подчинена правилам внутреннего контроля и требованиям регулятора. То есть организация обязана иметь обученных сотрудников и заложить в статьи расходов мероприятия по программе БОД, включая организацию защиты информации от несанкционированного взлома баз данных.

5.3.7.1. Проблемы России

Анализ финансовой системы страны предполагает обязательную оценку того, как внедряются рекомендованные FATF нормативы и стандарты Всемирного банка. Россия, например, про-

ходила оценку по методике ВБ в 2007 г. За время ее существования с 2001 г. проанализировано 67 стран мира.

Эксперты ВБ отмечают, что, несмотря на стремление многих стран к выполнению всех рекомендаций (40 рекомендаций FATF, 48 стандартов ВБ), в мире нет ни одной страны, которая могла бы сообщить о выполнении в полном объеме всех рекомендаций.

Так, России, например, была поставлена высшая оценка по п. 1 стандартов ВБ - у нас есть антиотмывочный закон. Россия также полностью выполняет п. 3 стандартов ВБ о конфискации преступных активов. А вот п. 5 (стандарт ВБ по внедрению банками внутренней политики «знай своего клиента») пока выполняется частично.

До сих пор не разработаны объединенные базы данных по преступникам. «Черный список» FATF стареет, и МВФ рекомендует FATF обновлять его. И потому любая организация, имеющая в перечне видов деятельности финансовые услуги, обязана выполнять весь комплекс мероприятий, направленных на БОД и БФТ, предписанных ФЗ № 115.

Как подчеркивают финансовые разведчики, такая мера - не следствие недоверия к тем или иным организациям, а в первую очередь защита их самих от использования лицами, занимающимися отмыванием и финансированием терроризма профессионально[98].

Подводя итог, необходимо отметить, что исследование терроризма требует инновационных методов, ибо в нем как нигде проявляется пароксистический, экстремальный конфликт прошлого с настоящим, а еще точнее, рудиментов традиционного мировоззрения с логикой современного мира.

При этом терроризм все активнее внедряет самые высокие технологии, опережая в том числе и используемые в госструктурах.

5.4. Кибероружие: реальны ли войны?

5.4.1. Особенности подходов и оценок США

В рамках совершенствования Национальной стратегии безопасности киберпространства США было проведено исследование потенциалов ряда стран относительно ведения информационных

[98] см. http://opec.ru/person.html?id=1306731

войн[99]. Исследование сосредотачивалось на оценке значения научно-технического и организационного потенциала в области ИКТ, способного привести к вторжению в критически важные компьютерные системы США, а также на изучении мотивов подобных действий со стороны суверенных государств.

Ранее для американских экспертов более характерным было изучение аналогичного потенциала террористических и экстремистских группировок, хакеров и их сообществ, но не суверенных государств. Кроме того, интересен перечень стран, представляющих угрозу безопасности США в киберпространстве: **Китай, Индия, Иран, КНДР, Пакистан, Россия**. В качестве стран, представляющих потенциальную угрозу для США, указаны **Израиль, Сирия и республики бывшей Югославии.**

Одним из выводов исследования является утверждение о том, что **процессы обработки информации являются важнейшей целью в современной войне.**

Характерным является также оцениваемая степень воздействия на информационную инфраструктуру США. По мнению экспертов, **реализация наиболее пессимистичного сценария, типа «электронного**
Перл-Харбора», в котором агрессор силами хакеров способен полностью вывести из строя сети связи и коммуникаций в США маловероятна.

Тем не менее, можно ожидать действий, способных скомпрометировать отдельные узлы корпоративных и государственных информационных сетей, ухудшить показатели качества связи, нарушить торгово-финансовые операции, спровоцировать сбои в критических системах. Речь идет о действиях, которые напрямую не могут быть квалифицированы как агрессия, но оказывают существенное влияние на управляемость государства, экономики и общества как в мирное, так и в военное время. Анализируя способности конкретных стран проводить подобные действия, авторы исследования отмечают следующее.

5.4.1.1. Китай

На сегодняшний день **Китай** в рамках программы трансформации своих вооруженных сил сформулировал официальное видение доктрины информационной войны, провел эксперименты по применению информационного оружия, а также ряд военных учений по

[99] См.http://netskop.ru/internet/news_2010-12-30-11-42-40-798.html

отработке принятой доктрины. Ведется подготовка специалистов в области информационных войн, включая подготовку офицерского состава. Разведывательные службы Пекина продолжают сбор научно-технической информации в интересах выполнения национального плана развития страны, в том числе и с активным использованием глобальных информационных сетей. Вооруженные силы Китая продолжают развивать связи с российскими военными и научными кругами, в том числе и по вопросам ведения информационных войн.

Вместе с тем американские эксперты отмечают стремление Китая развить его собственную уникальную модель ведения информационной войны, отражающую «китайскую специфику».

5.4.1.2 Индия

В последнее время индийское руководство стало уделять повышенное внимание вопросам ведения информационной войны, прежде всего в аспекте обеспечения собственных интересов в информационной сфере и обеспечением национальной безопасности. Причиной этого явились массированные атаки на индийские информационные системы, предпринятые группами пакистанских хакеров сразу после успешного испытания индийской атомной бомбы. Индийские власти объявили о внесении изменений в военную доктрину 1998 г., включив в нее вопросы радиоэлектронной борьбы и информационные операции. В среднесрочных планах развития страны особое внимание уделяется вопросам развития высокотехнологичных отраслей промышленности и информационных технологий. С целью поддержания высокого статуса индийских разработчиков информационных технологий на мировом рынке, планируется развитие сотрудничества правительственных структур и частного бизнеса. Кроме того, было создано разведывательное управление Минобороны, в рамках которого планируется создать агентство информационной войны с функционалом в области противодействия компьютерным нападениям, психологическим операциям, электромагнитному и инфразвуковому оружию.

5.4.1.3 Иран

В исследовании отмечается, что в последние месяцы все большее число американских экспертов в области национальной безопасности включают Иран в число стран, активизировавших деятельность в области подготовки к проведению информационных

операций. Так, за последние годы Тегеран стремится как можно выше поднять технологический уровень вооруженных сил не только созданием ядерного оружия, но и внедрением информатизированных образцов вооружения. В последнее время в стране создан целый ряд научно-исследовательских центров в сфере ИКТ, кроме того, Иран пытается приобретать на мировом рынке передовые разработки в области ИКТ. За последние годы укрепились связи Ирана с Россией и Индией, в их рамках осуществляется также подготовка специалистов в области информационных войн. В целом, эксперты отмечают, что Иран усиливает свои способности в секторе ИКТ как «фактора повышения боевой эффективности» с целью получить большее влияние в Центральной Азии.

5.4.1.4 Северная Корея

В отношении КНДР авторы исследования подчеркивают, что хотя эксперты и включают ее в список стран, которые смогут вести информационные войны (силами министерства обороны и специальных служб), доступные данные не содержат какой-либо информации о работах в Северной Корее в этом направлении. В ряде сообщений со стороны южнокорейских экспертов говорится о некоторых разведывательных операциях и взломах государственных информационных сетей в Республике Корея, предпринятых Пхеньяном, однако подобные свидетельства, скорее всего, носят дезинформационный характер. Вместе с тем, авторы полагают, что сегодня КНДР все же проводит эксперименты с некоторыми технологиями ведения информационной войны.

5.4.1.5. Пакистан

За последние годы получено немало официальных свидетельств активной деятельности групп пакистанских хакеров. Прежде всего, это проявилось в ходе масштабной кампании по взлому индийских информационных сетей после испытания Индией ядерного оружия. Эксперты склонны говорить о достаточно тесных связях пакистанских хакеров с государственными специальными службами. **Это позволяет считать, что Пакистан имеет достаточно разработанную доктрину информационной войны, особенно в плане проведения наступательных операций.**

Экспертами отмечается, что напряженные отношения Пакистана и Индии, наличие высококвалифицированного персонала в области ИКТ и покровительство со стороны правительственных

структур, создают благоприятную почву для интенсивного развития способностей в области наступательных приемов и методов информационной войны.

5.4.1.6. Россия

Американские эксперты отмечают, что Россия имеет достаточно эффективную доктрину информационной войны. Вооруженные силы России активно сотрудничают с экспертами в области ИКТ и академическими кругами с целью совершенствования ее приемов и методов. Кроме того, Россия наработала опыт в проведении информационных операций против чеченских информационных сайтов. Авторы также отмечают, что Россия продолжает проводить разведывательно-поисковые операции в государственных и частных информационных сетях США. **Вместе с тем, эксперты склонны считать, что специальные службы России или ее вооруженные силы в сегодняшних условиях не имеют мотивации к проведению скрытых дестабилизирующих действий в американских информационных системах и сетях.**

Резюмируя, эксперты подчеркивают, что за последнее время существенно возрос потенциал проведения информационных операций в отношении критически важных информационных систем США. Развиваются не только системы защиты информации, но и средства нападения, что приводит к существенному росту общего числа инцидентов в области компьютерной безопасности. В качестве основного вывода исследования, авторами рекомендуется руководству Министерства внутренней безопасности США предпринять дополнительные меры по усилению безопасности информационного пространства, прежде всего в массовом частном секторе и бизнес-секторе.

5.4.2. НАТО и кибербезопасность

На состоявшемся в ноябре 2010 г. в Лиссабоне саммите НАТО была принята новая Стратегическая концепция. Ее 12 пункт гласит, что **кибератаки могут дойти до черты, которая подвергает опасности национальное и евроатлантическое благосостояние, безопасность и стабильность. За такими атаками могут стоять иностранные ВС и разведки, организованная преступность, террористические и экстремистские группы**.

Ряд СМИ еще до принятия концепции сообщали, что группа экспертов во главе с бывшим госсекретарем США М.Олбрайт уделяет особое внимание кибербезопасности, поскольку этот вопрос стал приоритетным из-за роста уязвимости ключевых военных и гражданских инфраструктур, а также киберпространства стран-членов НАТО.

Следует отметить, что два государства-члена альянса США и Великобритания в последнее время начали создавать особые структуры по кибербезопасности, не входящие в состав министерства обороны или спецслужб, т.е. обладающие автономным статусом.

5.4.2.1. Cybercom США и Cyber Operations Group Великобритании

В июне 2009 г. министр обороны США заявил, что формируется особое объединение - Киберкомандование (Cyber Command, кратко - Cybercom). Минобороны США по некоторым оценкам насчитывает около 15 тыс.сетей, объединяющих 7 млн. компьютеров и других устройств в 88 странах мира[100] (известно, что в период с октября 2008 г. по апрель 2009 г. Пентагон потратил около $100 млн. на нейтрализацию ущерба от кибератак и решение различных проблем, возникших в сетях)[101].

В мае 2010 г. был назначен командующий Cybercom, генерал Кейт Александер, который с августа 2005 г. занимает должность директора агентства Национальной безопасности США (USA National Security Agency), специализирующегося на электронной разведке. Было объявлено, что в 2010-2015 гг. правительство США потратит на кибербезопасность $50 млрд.

В июне 2009 г. была опубликована «Стратегия кибербезопасности» Великобритании (UK Cyber Security Strategy)[102], согласно которой при британском правительстве был создан Офис кибербезопасности (Office of Cyber Security) и Центр действий кибербезопасности (Cyber Security Operations Centre). Годовой бюджет Офиса кибербезопасности был утвержден в размере 130 тыс.фунтов стерлингов, о бюджете Центра не сообщалось.

В 2010 г. были приняты новые варианты «Стратегии национальной безопасности» (National Security Strategy) и «Доклада стратегической обороны и безопасности» (Strategic Defense and Security

[100] http://noravank.am/rus/articles/derail.php?ELEMENT_ID=5292
[101] Без учета Wikileaks
[102] http://noravank.am/rus/articles/derail.php?ELEMENT_ID=5292

Review) Великобритании. Стратегия причислила атаки на британское киберпространство к числу угроз первого порядка, наряду с международным терроризмом, стихийными бедствиями и военными действиями между государствами. В докладе сообщалось о старте «Программы национальной кибербезопасности» (National Cyber Security Program), на осуществление которой в ближайшие четыре года будет выделено 630 млн.фунтов стерлингов. Кроме того, будет создана группа кибердействий (Cyber Operations Group), которая для решения своих задач должна консолидировать возможности государственного и частного секторов.

Вышеизложенное свидетельствует о том, что:

- кибербезопасность США и Великобритании становится стратегическим направлением, и именно этим обусловлено повышение статуса занимающихся кибербезопасностью органов в системах обеспечения национальной безопасности;
- в ближайшее время мы можем стать свидетелями появления в киберпространстве информационных кампаний нового уровня, в т.ч. хакерских атак нового типа, способных вывести из строя не только киберпространство противника, но и его критически важные инфраструктуры.

5.4.3. Боевой вирус Stuxnet: кибероружие против иранской ядерной программы

В конце сентября 2010 г. иранские власти официально признали, что компьютерные программы систем управления ядерных объектов (Бушерская АЭС и завод по обогащению урана в Натанзе), произведенные немецкой компанией Siemens, были подвергнуты атаке вирусом **Stuxnet**.

По данным ряда СМИ[103], Stuxnet был обнаружен в компьютерах, находящихся в Индии, Китае, Индонезии и Иране, однако, по оценке американской компании Symantec, около 60% вирусов Stuxnet были сосредоточены именно в Иране. **На иранских ядерных объектах Stuxnet вывел из строя около 30 тысяч компьютеров.** По данным компании VirusBlockAda (г.Минск), в обслуживаемых ею компьютерах в Иране вирус Stuxnet впервые был обнаружен еще 17 июня 2010 г., т.е. более, чем за два месяца до признания иранскими властями о нанесенном вирусом ущербе.

[103] См.http://www.computerra.ru/own/kiwi/564744/

Небезынтересен также модус действия Stuxnet. Вирус, внедрившись в компьютер (или в иное устройство), остается «спящим» до тех пор, пока не обнаружит отслеживаемый им код, который управляет определенным процессом (например, работой ядерного объекта). После этого Stuxnet, активизируется (в т.ч. по приказу «извне»), выводя из строя системы и одновременно передавая «наружу» информацию об объекте.

Представители Ирана не раз отмечали трудности борьбы с вирусом. Так, 27 сентября 2010 г. заместитель директора иранской Information Technology Company Х.Алипур заявил, что Stuxnet, помимо размножения, еще и мутирует (после его обнаружения начали распространяться три новых версии вируса). Тогда Алипур отметил, что потребуется два-три месяца до окончательного обезвреживания Stuxnet. Иран, не сумев одолеть вирус, стал нанимать в постсоветских странах и Восточной Европе экспертов для его уничтожения[104].

Официальный Тегеран заявил, что вирус не повлиял на деятельность Бушерской АЭС и других ядерных объектов. Однако факт, что после обнаружения вируса Иран был вынужден перенести с конца сентября до середины октября загрузку реакторов Бушерской АЭС ядерным топливом[105], а 16-22 ноября 2010 г. был остановлен действующий в Натанзе завод по обогащению урана, поскольку были зарегистрированы недопустимые колебания энергоснабжения центрифуги[106].

Министр разведки Ирана Г.Мослеи заявил (2 октября 2010 г.), что Stuxnet был послан врагом через Интернет с целью дезорганизации ядерной программы Ирана (т.е. Тегеран официально признал, что его ядерные инфраструктуры подверглись кибератаке). При этом официально так и не известно, какая страна(ы) или организация(и) стоят за Stuxnet. Что касается его создания и «доведения до цели», то рядовым хакерам это явно не под силу.

Согласно экспертным оценкам для того, чтобы Stuxnet смог воздействовать на иранские ядерные объекты еще на этапе его создания нужны были разведданные о software этих объектов.

---

[104] Погибший 29 ноября 2010 г. в Тегеране профессор по ядерной физике М.Шахриари, по информации израильских источников, возглавлял группу специалистов, ведущих борьбу с Stuxnet. В тот же день в результате другой атаки в Тегеране был ранен иранский профессор по ядерной физике Ф.Аббаси-Давани. После этого власти Ирана приняли решение усилить безопасность своих специалистов ядерной сферы.

[105] Согласно официальному иранскому объяснению, загрузка топлива была отложена из-за обнаруженной в одном из реакторов незначительной утечки.

[106] Об этом простое в Натанзе сообщил также директор МАГАТЭ (IAEA) Юкия Амано.

Кроме того, крайне важно довести вирус «до места назначения», что опять же из сферы деятельности спецслужб. В октябре 2010 г. органы иранской безопасности заявили о задержании нескольких «ядерных шпионов». 20 октября 2010 г. министр коммуникаций Ирана Р.Тапикур заявил, что в компьютерах ядерных объектов вирус распространялся также с помощью flash drivers («флешек»). При этом некоторые из распространителей делали это умышленно, другие же не знали, что их «флешки» содержат вирус Stuxnet.

Ряд публикаций[107] указывают на США и Израиль как на авторов Stuxnet и организаторов акций, отмечая, что это была попытка парализовать иранскую ядерную программу без применения военной силы и оказать психологическое давление на Иран. Вбрасывалась также мысль, что в акции могли участвовать и российские спецслужбы, поскольку большинство иностранцев, работающих на иранских ядерных объектах, являются россиянами. В качестве обоснования этой точки зрения отмечаются известные российско-иранские противоречия вокруг иранской ядерной программы, в результате которых Россия отказалась продать Тегерану комплексы противовоздушной обороны С-300. Кроме того, по сообщениям ряда СМИ, во время следствия, проведенного иранскими органами безопасности в связи с Stuxnet, были допрошены работающие в Иране российские специалисты и члены их семей.

Таким образом, главное - это не выявление страны или организации, организовавшей Stuxnet, а то, что посредством кибератаки де-факто возможно уничтожение ключевых инфраструктур государства. Одновременно США и Великобритания создали органы кибербезопасности нового уровня.

Характерна оценка директора центра национальной кибербезопасности и интеграции коммуникаций США, которую он озвучил 17 ноября 2010 г. во время слушаний в Сенате США**: Stuxnet «изменил правила игры», и такой вирус может вывести из строя жизненно важные для государств инфраструктуры, повредить распределительные сети электроэнергии и питьевой воды, работающие по компьютерным программам заводы и т.д.**

5.4.4. Инсайдер–Герострат, или уроки Wikileaks

Беспрецедентная публикация сотен тысяч закрытых документов дипломатической переписки США на сайте WikiLeaks, а также

[107] http://www.computerra.ru/own/kiwi/565316/

в солидных изданиях вызвала у политического истеблишмента всего мира сначала замешательство, а затем массу споров и противоречий, в т.ч. судебных и моральных.

Особую пикантность проблеме придало то обстоятельство, что некоторые из документов были написаны совсем недавно, в конце февраля 2010 г. и содержат взгляд администрации Б.Обамы на кризисы и конфликты в мире.

В силу этого госсекретарь США Х.Клинтон и американские послы во всем мире связывались с официальными лицами других стран, чтобы предупредить о раскрытии информации. В заявлении Белого дома сказано: «Мы самым решительным образом осуждаем несанкционированное разглашение секретных и чувствительных для национальной безопасности документов. Президент Б.Обама поддерживает ответственность, подотчетность и открытость правительства дома и по всему миру. Но это безрассудное и опасное деяние противоречит этой цели. Выпуская украденные секретные документы, WikiLeaks поставило под угрозу не только дело защиты прав человека, но и жизнь и работу этих лиц».[108]

Выборки из переписки между Госдепом США и почти 270 посольствами и консульствами составляют секретную хронику отношений между США и миром в отношении войны и терроризма. Среди них откровения, которые были опубликованы в т.ч. в «The Times»:

1. **Опасное противостояние с Пакистаном из-за ядерного топлива**. Начиная с 2007 г., США в тайне предпринимали усилия, до сих пор неудачные, по удалению обогащенного урана из пакистанского исследовательского реактора, чтобы предотвратить его использование в незаконных ядерных устройствах. В мае 2009 г. американский посол в Пакистане Э.Паттерсон сообщила, что график посещения страны американскими экспертами сорван. Пакистанская сторона сообщила, что «если в мировые СМИ попадет информация о перемещении ядерного топлива, то они скажут, что США забирает у Пакистана ядерное оружие».

2. **Моделирование вероятного падения режима в Северной Корее**. Американские и южнокорейские официальные лица обсудили перспективы объединения Кореи: смогут ли экономические и политические проблемы привести к взрыву в этой стране. Южнокорейцы даже считаются с экономическими интересами Китая в Корее. Американский посол в Сеуле сообщила в Вашингтон в феврале (2010 г.), что южнокорейские официальные лица верят, что пра-

[108] См. http://digest.subscribe.ru/economics/expres/n418669393.html

вильные деловые договоренности об отношениях с объединенной Кореей положат начало альянсу с США.

3. **Гуантанамо**. Когда американские дипломаты под давлением мировой общественности переселяли пленников, они невольно стали фигурами в игре Госдепа США под названием «Давайте договоримся». Словения сказала, что примет заключенных, если это поможет встрече с президентом Б.Обамой. Островному государству Кирибати были предложены миллионы долларов, чтобы те приняли китайских мусульман. Также американцы предположили, что если Бельгия примет больше пленных, то это поможет ей стать более значительной в Европе.

4. **Афганистан**. Подозрение в коррупционности правительства. Когда вице-президент Афганистана посетил ОАЭ в прошлом году, местные органы по борьбе с наркотиками обнаружили, что он нес 52 млн.долларов наличными. В американском сообщении из Кабула говорилось о «значительной сумме», происхождение которой чиновнику А.Зие Массуду удалось скрыть (г-н Масуд отрицает принятия каких-либо деньги из Афганистана.)

5. **Глобальная хакерская угроза**. Китайское Политбюро санкционировало взлом серверов Google. Об этом сообщили американскому посольству в Пекине. Взлом серверов Google был частью компании по компьютерному саботажу, которым занимались правительственные структуры, частные эксперты по защите и Интернет-преступники, завербованные китайским правительством. Они взломали компьютеры американского правительства и их союзников, сообщается в секретном документе.

6. **Комплекс сообщений по терроризму**. Саудовские доноры по-прежнему являются главными финансистами суннитских вооруженных группировок, таких как Аль-Каида. И крошечное государство Катар в Персидском заливе, которое является опорой американских военных на протяжении многих лет, явилось «худшим в регионе» по борьбе с терроризмом. Спецслужбы Катара опасаются действовать против известных террористов, чтобы не спровоцировать репрессии.

7. **Интригующий альянс**. Американские дипломаты в Риме сообщили, что их итальянский контактер описывает как экстраординарный факт отношения между итальянским премьером С.Берлускони и российским главой правительства В.В.Путиным. В сообщении говорится, что С.Берлускони «все больше является рупором Путина в Европе». Дипломаты также отметили, что В.В.Путин пользуется превосходством над всеми другими политическим деятелями в России, но его позиция расшатывается не-

управляемой бюрократией, которая часто игнорирует его распоряжения.

8. **Поставка оружия боевикам**. Источник описывает отсутствие противодействия США в поставках Ливаном оружия террористам «Хезболлах». Президент Сирии обещал Госдепу, что «он не будет посылать новое оружие «Хезболлах». Однако есть информация о том, что Сирия продолжает поставки вооружений.

В информации ВВС со ссылкой на «The Guardian», сообщается:

- об утверждениях относительно связей российских властей с оргпреступностью;
- о попытках Ирана переоборудовать северокорейские ракеты для использования в качестве ракет дальнего радиуса действия;
- об американских чиновниках, которым приказывали следить за руководством ООН;
- о критике британских политиков, в том числе премьер-министра Д.Кэмерона;

«The Guardian» сообщает, что среди обнародованных 3376документов большинство относятся к американскому посольству в Москве[109].

Резюмируя, следует отметить, что системой SIPRnet[110], через которую произошла утечка информации, пользуется широкий круг людей, так как при ее помощи осуществляется обмен закрытой информацией уже более десяти лет. В силу этого необходимо подчеркнуть, что с данными об источниках информации должны были обращаться более осторожно.

Бывший директор ЦРУ Хэйден отметил, что правила, в соответствии с которыми действует Пентагон, могут отличаться от правил, которыми руководствуется ЦРУ. Вместе с тем, по его мнению, с одной стороны, необходимо обеспечивать защиту источников развединформации, а с другой стороны, тем, кто анализирует эту информацию, необходимо знать, от кого она получена, с тем, чтобы оценить ее достоверность. Эти соображения трудно сбалансировать.

По словам руководителя отдела тактической разведки частной фирмы Stratfor С.Стюарта, никого не удивляет, когда многие из сообщений и докладов содержат имена конкретных людей.

Согласно сообщениям представителей Талибана, они изучают документы, опубликованные на WikiLeaks, чтобы найти тех, кто помогал войскам США.

---

[109] http://www.ng.ru/newsng/2010-11-29/100_wikileaks.html

[110] См. Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности. М.: Парад, 2005. С.124

Разглашение секретных сведений об Афганской войне может обернуться гибелью военнослужащих коалиции и афганских граждан. Такое мнение высказал председатель Объединенного комитета начальников штабов ВС США адмирал М.Маллен. Он сказал, что уже имеются сведения о том, что лидеры Талибана распорядились составить список информаторов войск коалиции, чьи имена фигурируют в десятках тысяч документов, выставленных на сайте WikiLeaks. По словам М.Маллена, публикация такого массива военной информации не имеет прецедентов.

Министр обороны США Р.Гейтс назвал утечку сведений результатом потери «морального компаса».

Характерно, что одним из факторов мятежа в Тунисе (январь 2011 г.) стала информация WikiLeaks о коррупции в высших органах госвласти страны.

В связи с уголовным преследованием основатель сайта WikiLeaks Д.Ассанж сказал[111] об имеющихся у него «страховочных» документах, которые он приберег для публикации на случай, если с ним или его ресурсом что-нибудь случится. Интервью Д.Ассанжа опубликовано в журнале «The New Statesman», вышедшем 13 января 2011 г.

Содержания этих файлов Д.Ассанж не раскрыл, однако отметил, что опасаться стоит не только правительству США, но и медиамагнату Руперту Мердоку. По словам основателя WikiLeaks, у него есть 504 дипломатические депеши, касающиеся Р.Мердока и его корпорации «News Corp». Заявление Д.Ассанжа прозвучало на фоне высказываний его адвокатов о том, что ему может грозить смертная казнь в случае экстрадиции в США. В то же время основателя сайте WikiLeaks, который сейчас находится в Великобритании, могут выдать Швеции, где он обвиняется в преступлениях сексуального характера. Слушания по делу об экстрадиции назначены на февраль 2011 г.

В начале декабря 2010 г. WikiLeaks уже рассказывал о своей подстраховке. В случае, если бы Д.Ассанж попал под арест или был убит, ресурс пообещал раскрыть все имеющиеся у него секретные документы. Для этого ранее в файлообменные сети был выложен файл insurance.aes256 размером в 1,4 гигабайта, который, как предполагается, содержит депеши американских дипломатов. Файл зашифрован ключом из 256 цифр, который и будет опубликован в случае неприятностей с Д.Ассанжем.

[111] http://news.rambler.ru/8688272/13.01.2011

Из инцидента с WikiLeaks уроки извлекают многие страны. В этом контексте для России важным шагом стало принятие Федерального закона № 224-ФЗ от 27 июля 2010 г. «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» (основные положения ФЗ вступают в силу через 180 дней после подписания).

Данный ФЗ направлен на создание эффективного механизма для выявления и пресечения правонарушений, совершаемых путем использования инсайдерской информации и манипулирования рынком.

Согласно закону, под инсайдерской понимается точная и конкретная информация, в том числе сведения, составляющие коммерческую, служебную, банковскую тайну и тайну связи, распространение или предоставление которой может, в частности, оказать существенное влияние на цены финансовых инструментов, иностранной валюты или товаров.

Законом определяется также круг инсайдеров и перечень действий, относящихся к манипулированию рынком. Расширяются полномочия федерального органа исполнительной власти в области финансовых рынков, в частности, ему предоставляется право проводить проверки, получать объяснения, требовать предоставления документов и информации, направлять предписания об устранении нарушений.

Также ФЗ обязывает соответствующие организации принять внутренние правила доступа к инсайдерской информации в целях ее охраны, а также назначить должностных лиц, отвечающих за осуществление такого контроля. Кроме того, предусматривается введение мер уголовной и административной ответственности за манипулирование рынком, неправомерное использование инсайдерской информации, в том числе в виде взыскания в доход государства всей суммы излишнего дохода либо суммы убытка, которого удалось избежать в результате неправомерного использования инсайдерской информации

Президент России Д.А.Медведев обратил особое внимание на то, что при использовании нового закона «должен быть настоящий, разумный баланс между, с одной стороны, недопустимостью противоправного использования инсайдерской информации, а, с другой стороны, защитой свободы слова и возможностью использования экономической информации, которая получается из установ-

ленных законом источников правомерным образом и используется в соответствии с этим законопроектом».

Беспрецедентные уроки WikiLeaks императивно диктуют необходимость принятия соответствующих, в первую очередь превентивных, мер и на всех других треках борьбы с инсайдерами.

ВМЕСТО ЗАКЛЮЧЕНИЯ

Политик должен уметь предсказать,
что произойдет завтра, через неделю,
через месяц и через год. А потом объяснить,
почему этого не произошло.

У. ЧЕРЧИЛЛЬ

Методологии форсайта, интегрального макропрогнозирования глобальной безопасности или…?

Кроме рассмотренных в предыдущих главах инновационных методов анализа глобальной безопасности в последнее время к таковым относят также **методологии форсайта**[112] **и интегрального макропрогнозирования.** Рассмотрим их суть.

Появившись около 30 лет назад, форсайт стал одним из основных инструментов инноватики. **Методология форсайта ориентирована на определение возможных вариантов будущего, вобрав в себя десятки традиционных и достаточно новых экспертных методик.** Основной вектор методологии направлен на более активное и целенаправленное использование знаний экспертов. Обычно **в каждом из форсайт-проектов применяется комбинация различных методов, в числе которых экспертные панели, Дельфи (опросы экспертов в два и более этапа), SWOT-анализ**[113]**, мозговой штурм, построение сценариев, технологические дорожные карты, деревья релевантности, анализ взаимного влияния и др**. Для учета самых различных вариантов и получения полной картины привлекается значительное число участников. Так, в японских долгосрочных прогнозах научно-технологического развития, проводимых каждые пять лет, участвует более 2-х тысяч

[112] Форсайт (от англ. Foresight - «взгляд в будущее») – эффективный инструмент формирования приоритетов и мобилизации большого количества участников для достижения качественно новых результатов в сфере науки и технологий, экономики, государства и общества. По результатам форсайт-проектов создаются дорожные карты. Является одним из важнейших инструментов инновационной экономики.

[113] SWOT - метод анализа в стратегическом планировании, заключающийся в разделении факторов и явлений на четыре категории: strengths (сильные стороны), weaknesses (слабые стороны), opportunities (возможности) и threats (угрозы).

экспертов, а в недавнем корейском проекте участвовали свыше 10 тысяч экспертов[114].

Форсайт ориентирован не только на определение возможных альтернатив, но и на выбор оптимальных из них. В процессе выбора применяются различные критерии для определения наиболее предпочтительных вариантов. Форсайт исходит из того, что наступление «желательного» варианта будущего во многом зависит от действий, предпринимаемых сегодня, поэтому их выбор сопровождается разработкой мер, обеспечивающих оптимальную траекторию инновационного развития.

Большинство форсайт-проектов в качестве центрального компонента включают перспективы развития науки и технологий. Обычно эти вопросы становятся предметом обсуждения не только ученых, но и политиков, экспертов из разных отраслей экономики. Сама организация систематических попыток «заглянуть в будущее» приводит к формированию более высокой культуры управления и в итоге - к формированию более обоснованной инновационной политики.

Форсайт-проекты ориентированы не только на получение нового знания в форме докладов, набора сценариев, рекомендаций и т.п. В ряде проектов формирование горизонтальных сетей, площадок, в которых ученые и бизнесмены, преподаватели вузов и чиновники, специалисты смежных областей могут обсуждать общие проблемы, рассматривается как один из главных эффектов.

В соответствии с Руководством по стратегическому форсайту (П.Бишопа) существует 5 его этапов[115]:

- **Формирование объекта**, т.е. сферы проведения форсайта: ИКТ, космос, нанотехнологии и т.д. В политическом форсайте объект конструируется специально.
- **Формирование существенных условий** - целевых показателей, которых мы хотим достигнуть в будущем. Для форсайта принципиальным является то, чтобы существенные условия отражали качественное изменение (например, повышение уровня информационной безопасности) и имели количественное выражение.
- **Сканирование** - т.е. формирование «карты сферы» -(стейкхолдеры, эксперты, компании), выбор методов исследования и проведение экспертных опросов.

[114] См. http://ru.wikipedia.org/wiki/%D0%A4%D0%BE%D1%80%D1%81%D0%B0%D0%B9%D1%82

[115] .См. http://ru.wikipedia.org/wiki/%D0%A4%D0%BE%D1%80%D1%81%D0%B0%D0%B9%D1%82

- **Альтернативы будущего** - выделение тенденций, которые можно спрогнозировать, выявление зон неопределенности и формирование возможных сценариев будущего.
- **Планирование и исполнение** - разработка и создание дорожных карт, включение всех стейкхолдеров в обсуждение будущего, изменение стратегии и действий заказчика форсайта (изменение стратегии, формирование новых проектов и программ).

Опыт форсайт-проектов западных стран показывает, что, в первую очередь, необходимо ответить на вопрос: чего мы хотим достигнуть в будущем, к чему необходимо прилагать усилия. Это связано с тем, что такие понятия, как качество жизни, уровень доверия, гражданское общество и т.д., являются социокультурными феноменами, они не существуют объективно, а формируются как эффект определенной практики. В политических форсайт-проектах этот этап выделяется в отдельный и называется выработкой «существенных условий».

Как правило, форсайт-проекты проводятся регулярно, иногда по повторяющейся схеме (в Японии - каждые 5 лет, начиная с 1971 г.), в других случаях исследования проводятся как взаимосвязанные проекты, нацеленные на решение комплекса задач и формирование согласованного представления о долгосрочных перспективах развития технологий, инноваций и социума, в т.ч. глобального.

Другим направлением анализа глобального развития является **школа интегрального макропрогнозирования**. Она интегрирует, развивает и применяет результаты ряда научных школ: русского циклизма, цивилизационной, ноосферной. Как подчеркнул в интервью председатель Отделения циклов и прогнозирования Российской академии естественных наук (РАЕН) профессор Ю.В.Яковец (16.12.2010 г.)[116], объединение понятий **интегрального и макропрогнозирования** имеет глубокий смысл. **Интегральный** - потому что здесь синтезируются и системно развиваются несколько направлений прогностической мысли:

- Теория предвидения и учение о циклах, кризисах и инновациях Н.Кондратьева, С.Кузнеца, Й.Шумпетера.
- Цивилизационный подход к прошлому, настоящему и будущему человечества и учение о социокультурной динамике П.Сорокина, А.Тойнби и Ф.Броделя.
- Учение о ноосфере, коэволюции общества и природы В.Вернадского и Н.Моисеева.
- Балансовый метод макропрогнозирования В.Леонтьева.

[116] http://www.raen.info/press/faces/document3401.shtml

Это позволяет отразить многомерность окружающего нас мира и происходящих в нем глубоких трансформаций, получить объемное видение будущего.

Предметом исследования макропрогнозирования являются не отдельные отрасли и направления изменений в обществе и природе, а перемены высшего уровня и наибольшей глубины, предопределяющей динамику общества в целом, в его глобальном и национальном измерениях.

Интеграция двух подходов отличает данную методологию от преобладающей **ныне методологии форсайта. При этом, чем больше экспертов вовлечено в процесс предвидения, тем больше доминирует сила инерции мышления, для которого непривычны крутые изломы, точки бифуркации, кризисы и революции.** Пониманием циклично-генетических закономерностей владеют пока немногие ученые.

Другая особенность - **междисциплинарный** характер исследований, в которых объединены ученые самых разных специальностей: экономисты и социологи, историки и философы, экологи и математики, причем из разных стран.

Точкой отсчета в формировании методологии интегрального макропрогнозирования можно считать проведение междисциплинарных дискуссий по проблемам теории циклов, макропрогнозирования, стратегического планирования, инноваций с Президентом РАЕН, профессором О.Л.Кузнецовым еще в 1988 г. С тех пор состоялось 27 таких дискуссий. В 1990 г. в ходе 3-й дискуссии была создана Ассоциация «Прогнозы и циклы», в 1992 г. - Международный фонд Н.Д.Кондратьева. В 1996 г. сформировано Отделение исследования циклов и прогнозирования РАЕН. В 1999 г. создан Международный институт П.Сорокина - Н.Кондратьева. Подготовлен проект Международного центра интегрального макропрогнозирования, стратегического планирования и инновационного программирования (проект был отмечен специальным призом в рамках «ЭКСПО-2010»). Образован подкомитет «Стратегическое планирование и прогнозирование» в составе Комитета торгово-промышленной палаты России по содействию модернизации и технологическому развитию.

Следует отметить также выход в свет таких работ, как «Закономерности научно-технического прогресса и их планомерное использование», «Теория предвидения: парадигма цикличности» (1991), «История цивилизаций» (1995, 1997), «Циклы. Кризисы. Прогнозы» (1999), «Русский циклизм: новое видение прошлого и будущего» (1999, издана в США), «The Past and the Future of

Civilizations» (2000, США), «Эпохальные инновации XXI века» (2004), «Глобальные экономические трансформации XXI века» (2010), «Россия - 2050: стратегия инновационного прорыва» (2004, 2005), семитомник «Цивилизации: теория, история, диалог, будущее» (2006-2010). Крупным достижением стало международное исследование (в 2007-2009 гг.) «Будущее цивилизаций» на период до 2050 года, опубликованное в 10 частях. В его подготовке приняли участие более 70 ученых из России, Казахстана, Украины, США, Ливана и других стран[117].

Данная научная школа была представлена на заседании Круглого стола «Будущее цивилизаций и стратегия цивилизационного партнерства» в рамках 64-й сессии Генассамблеи ООН 27 октября 2009 г. В настоящее время подготовлен проект Всеобщей декларации ЮНЕСКО о стратегии диалога и партнерства цивилизаций в области науки, образования, культуры и этики для обсуждения на V Цивилизационном форуме в ЮНЕСКО в сентябре 2011 г.

Опубликован доклад «Стратегия глобального устойчивого развития на базе партнерства цивилизаций» для обсуждения на Круглом столе в ООН в апреле 2011 г. в рамках 65-й сессии Генассамблеи ООН и на VI Цивилизационном форуме в рамках Всемирного саммита в Бразилии «РИО+20» в 2012 г.

Методика интегрального макропрогнозирования лежит в основе разрабатываемого Координационным советом РАН по прогнозированию перспектив научно-технологического и социально-экономического развития России на период до 2030 года[118]. В этом контексте перспективен метод стратегических матриц, разработанный Институтом экономических стратегий во главе с действительным членом РАЕН, доктором экономических наук, профессором А.И.Агеевым (см. § 4.4).

Вместе с тем, анализ достижений отечественных научных школ на треке исследования проблем глобальной безопасности и прогнозирования показывает, что в них недооценивается стремительно растущий потенциал ИКТ, в т.ч. суперкомпьютеров[119] и информационно-аналитических программ нового поколения, включая обучаемые нейронные сети (см. § 4.2)**.**

---

[117] См. www.newparadigm.ru

[118] http://www.rusfuture.newparadigm.ru/files/10_07_29_sit_analis_part_1.pdf

[119] Суперкомпьютер (англ. *supercomputer*, СуперЭВМ) - вычислительная машина, превосходящая по своим техническим параметрам большинство компьютеров. Современные суперкомпьютеры представляют собой большое число высокопроизводительных серверных компьютеров, соединенных друг с другом локальной

Именно по этому пути идут ведущие страны мира. В России на это нацелена государственная программа «Информационное общество (2011-2020 годы)», утвержденная Распоряжением Правительства РФ № 1815-р от 20.10.2010 г.

Однако, как показывает практика, одной стране, даже с очень развитой и высокотехнологичной экономикой, справиться со столь масштабными вызовами и глобальными угрозами не по плечу. Вот почему Россия выступила инициатором заключения Соглашения между Российской Федерацией и Европейским Союзом о сотрудничестве в сфере кризисного регулирования (проект см. в Приложении).

Рассмотреть весь обширный спектр инновационных методов анализа глобальной безопасности в одной работе, естественно, невозможно. В силу этого коллектив авторов намерен продолжить столь важное для судеб России и цивилизации дело и приглашает к взаимополезному сотрудничеству всех экспертов по данной проблематике, в том числе в рамках Национального института исследований глобальной безопасности[120].

высокоскоростной магистралью для достижения максимальной производительности в рамках подхода распараллеливания вычислительной задачи

[120] Подробнее о Национальном институте исследований глобальной безопасности см. на www.niiglob.ru

ГЛОССАРИЙ

При составлении глоссария были использованы следующие источники: Стратегия национальной безопасности Российской Федерации до 2020 года (утв. Указом Президента 12.05.2009 г. № 537), Военная доктрина Российской Федерации (утв. Указом Президента 05.02.2010 г. № 146), а также труды авторов, перечисленных во введении к данной книге.

Аппаратная закладка - специальное электронное устройство перехвата информации, скрытно встраиваемое или подключаемое к техническим средствам объекта информатизации (сети передачи данных) в целях несанкционированного получения защищаемой информации.

Атака Ethernet контролируемая - форма *атаки информационной*, направленной на основной поток сообщений в сети Ethernet (например, контролируя пачки, проходящие через маршрутизатор) и изменение порядка дальнейшего движения для сообщений определенного вида или с определенными признаками (например, содержащими конкретный пароль).

Атака активная - форма нападения на *ресурс информационный*, в результате которого фактически изменяются или уничтожаются хранимые или обрабатываемые в нем данные или другие элементы ресурса.

Атака асинхронная - форма *атаки информационной*, при которой используются преимущества динамических действий системы, особенно способность управлять выбором времени исполнения тех или иных действий.

Атака информационная (нападение, кибератака) - попытка предпринять *действия несанкционированные* в системе (сети) в обход или с разрушением средств защиты. *Нападение активное* нарушает (изменяет или уничтожает) данные. *Нападение пассивное* освобождает (снимает ограничения доступа) данные.

Атака хакерская - атака на *систему информационную* (сеть) или какую-либо ее часть, выполненная отдельным лицом (хакером) или согласованной группой лиц. Наиболее часто используется тактика, которая позволяет *злоумышленнику* узурпировать сессию *пользователя уполномоченного* для собственных, как правило, криминальных целей.

Баланс сил (англ. balance of power) - ключевое положение в теории политического реализма, обозначающее ситуации равновесия между государствами. Может рассматриваться и как результат действия национальных правительств, и как порядок в международных отношениях, не зависящий от политиков. Концептуально восходит к работам Фукидида, но распространение получает с XVIII в., особенно при анализе британской и обще-

европейской политики между войнам Наполеона I и Первой мировой войной. Это положение основано в том числе на трактовке Гоббсом международных отношений как враждебной, анархической среды, в которой государства постоянно подвержены угрозе нападения и вынуждены поддерживать соизмеримый с соперниками силовой потенциал.

Безопасность глобальная (международная) - состояние отношений между государствами мира, при котором им не угрожает опасность военной, экономической, любой другой экспансии, посягательство извне на существование, суверенное и независимое прогрессивное развитие. Уставом Организации объединенных наций (ООН) главная ответственность за поддержание международного мира возложена на Совет безопасности ООН.

Безопасность информационная - 1) состояние защищенности основных интересов личности, общества и государства в информационном пространстве, включая *инфраструктуру информационно-телекоммуникационную* и собственно информацию в отношении таких ее свойств, как целостность, объективность, доступность и конфиденциальность; 2) совокупное состояние: а) пространства информационного, при котором обеспечивается его формирование и развитие в интересах граждан, организаций и государства; б) инфраструктуры информационной, при котором информация используется строго по назначению и не оказывает негативного воздействия на систему (объект) при ее использовании; в) информации, при котором исключается или существенно затрудняется нарушение таких ее свойств, как конфиденциальность, целостность и доступность; 3) защищенность информационной среды личности, общества и государства от преднамеренных и непреднамеренных угроз и воздействий.

Безопасность информационная международная - состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в пространстве информационном.

Бихевиоризм (англ. behavio(u)rism от behaviour - поведение) - ведущее направление американской экспериментальной психологии XX в., идеи и методы которого были перенесены в 1950-1960-х годах в политологию. Для современных бихевиористских концепций политики характерен акцент на изучении ее микроповеденческих сторон, различных механизмов индивидуального, межличностного и группового политического поведения. Бихевиористскому методу в политологии присуща отчетливая прикладная ориентация.

Бомба двойная (вилочная) - разрушающий программный элемент, применяемый в основном к Unix-основанным системам, который инициирует безудержный процесс разделения и повторения (копирования) операционных процессов, что приводит к деградации производственных возможно-

стей системы или (если насыщенность достигнута) полностью исключает возможность нормального функционирования системы.

Бомба логическая - обобщающий термин деструктивных программных комплексов (см.: вирус программный, троянский конь, часовая мина), резидентно находящихся на компьютере «жертвы» и активирующихся по определенному логическому условию (например, достижение определенной даты или набора определенных состояний системы). Наиболее известным и распространенным является срабатывание логической бомбы на заранее заданный контекст (ключевое слово). Может быть самостоятельной программой или фрагментом кода, распространяемым программистами или производителем некоторого программного продукта (пакета программ). Используется для инициирования вирусной или иного рода программной атаки на компьютерную систему. Механизм разрушающего воздействия может быть сколь угодно различным.

Бомба почтовая (Бомба-письмо) - деструктивный программный комплекс, способный передаваться с почтовыми (e-mail) сообщениями и активироваться на сервере или рабочей станции адресата. Как правило, нацелены на уничтожение информации на рабочей станции, но существуют примеры для нарушения работы сетей или отдельных их элементов. Чаще используется в Unix-основанных системах.

Борьба радиоэлектронная (РЭБ) - любые военные действия, связанные с использованием электромагнитной и направленной энергии, в целях контроля над средствами электромагнитного спектра или нападения на противника. К трем главным подразделам РЭБ относятся нападение радиоэлектронное, защита радиоэлектронная, поддержка средствами РЭБ.

Версальско-вашингтонская система международных отношений - миропорядок, основы которого были заложены Версальским мирным договором 1919 г., договором с союзниками Германии, а также соглашениями, заключенными на Вашингтонской конференции 1921-1922 гг. Европейская часть этой системы (иначе - *Версальская)* в значимой мере была создана под влиянием политических и военно-стратегических соображений стран-победительниц при игнорирования интересов побежденных и вновь образованных стран (в Европе - 9), что делало эту структуру уязвимой из-за требований ее преобразования и не способствовало долговременной стабильности в мировых делах. Отказ США от участия в функционировании Версальской системы, изоляция России и антигерманская направленность превращали ее в несбалансированную и неуниверсальную, что увеличивало потенциал будущего мирового конфликта. *Вашингтонская* система, распространяющаяся на АТР, отличалась несколько большим равновесием, но тоже была неуниверсальной. Ее нестабильность обусловливали неопределенность политического развития Ки-

тая, милитаристский внешнеполитический курс Японии и изоляционизм США.

Вирус программный - обобщенный термин, определяющий фрагмент программного кода, способный самокопироваться («размножаться») путем записи своей копии в коды других программ компьютерной системы, подвергающейся компьютерному проникновению, разработанный для негативного воздействия на информацию или программное обеспечение компьютерной системы, скрываясь как часть другой программы. Активируется при запуске программы, в которую он внедрен, после чего может либо скопировать себя в другую программу, либо выполнить действия по искажению данных или нарушению работоспособности системы. Отличается способностью передаваться с другими программами практически любых видов, часто способностью самокопирования и в других системах, с которыми инфицированная система взаимодействует.

Военная безопасность Российской Федерации - состояние защищенности жизненно важных интересов личности, общества и государства от внешних и внутренних военных угроз, связанных с применением военной силы или угрозой ее применения, характеризуемое отсутствием военной угрозы либо способностью ей противостоять.

Военная опасность - состояние межгосударственных или внутригосударственных отношений, характеризуемое совокупностью факторов, способных при определенных условиях привести к возникновению военной угрозы.

Военная организация государства - совокупность органов государственного и военного управления, Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, составляющих ее основу и осуществляющих свою деятельность военными методами, а также части производственного и научного комплексов страны, совместная деятельность которых направлена на подготовку к вооруженной защите и вооруженную защиту Российской Федерации.

Военная политика - деятельность государства по организации и осуществлению обороны и обеспечению безопасности Российской Федерации, а также интересов ее союзников.

Военная угроза - состояние межгосударственных или внутригосударственных отношений, характеризуемое реальной возможностью возникновения военного конфликта между противостоящими сторонами, высокой степенью готовности какого-либо государства (группы государств), сепаратистских (террористических) организаций к применению военной силы (вооруженному насилию).

Военное планирование - определение порядка и способов реализации целей и задач развития военной организации, строительства и развития Вооруженных Сил и других войск, их применения и всестороннего обеспечения.

Военный конфликт - форма разрешения межгосударственных или внутригосударственных противоречий с применением военной силы (понятие охватывает все виды вооруженного противоборства, включая крупномасштабные, региональные, локальные войны и вооруженные конфликты);

Военный конфликт - форма разрешения межгосударственных или внутригосударственных противоречий с применением военной силы (понятие охватывает все виды вооруженного противоборства, включая крупномасштабные, региональные, локальные войны и вооруженные конфликты).

Воздействие информационное - акт применения информационного оружия, а также непосредственное воздействие на элементы информационного пространства противника иными методами с целью нанесения ущерба.

Воздействие информационно-психологическое - психологические действия, осуществляемые с прямым или опосредованным использованием информационно-психологических средств.

Воздействие информационно-энергетическое - воздействие на биосистемы, и прежде всего на человека, физических полей различной природы, модулированных семантическими (смысловыми) сигналами, воспринимаемое биологическими организмами, а также средой их обитания в форме сигналов, сообщений, сведений, образов (т.е. в виде информации).

Воздействие на информационное пространство силовое - нарушение с использованием *оружия информационного* нормального (установленного законными собственниками, владельцами и пользователями) функционирования *инфраструктуры общества информационной*, правил формирования, хранения и распространения информации и информационных ресурсов.

Воздействия информационного средства - 1) совокупность специальных лингвистических, программных, технических и иных средств, обеспечивающих извлечение, искажение или разрушение *информации*, *потоков информационных* или *ресурсов информационных;* 2) в информационных операциях эффективное использование *информации*, *систем информационных* и технологий в целях усиления средств и сил при осуществлении стратегии *операций информационных.*

Война - конфликт между политическими образованиями (государствами, племенами, политическими группировками и т.д.), происходящий в форме боевых действий между их вооруженными силами. Как правило, война имеет целью навязывание оппоненту своей воли. По формулировке

Клаузевица, «война есть продолжение политики иными средствами». Основным средством достижения целей войны служит организованная вооруженная борьба как главное и решающее средство, а также экономические, дипломатические, идеологические, информационные и другие средства борьбы. В этом смысле война - это организованное вооруженное насилие, целью которого является достижение политических целей.

Война информационная - (Война третьей волны, Война знаний, Война постиндустриальная, Война информационно-основанная) 1) *противоборство информационное* между государствами в *пространстве информационном* с целью нанесения ущерба *системам информационным*, процессам и ресурсам *структур критически важных*, подрыва политической, экономической и социальной систем, а также массированной психологической обработки населения с целью дестабилизации общества и государства; 2) особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, средства и технологии *силового воздействия на информационную сферу* этих государств. Выделяются следующие разновидности *войны информационной:* а) подавление и уничтожение систем управления противоборствующей стороны, информационное обеспечение боевых действий, электронное подавление, психологическое воздействие, хакерская война, война в области экономической информации и кибернетическая война; б) подавление и уничтожение систем управления противоборствующей стороны - направлено на физическое уничтожение командных пунктов противника, нарушение управления его силами и средствами; в) информационное обеспечение боевых действий - нацелено на максимально полное предоставление и использование в системах управления войсками и оружием информации, собираемой интегрированными информационными системами в ходе военных действий; г) электронное подавление - имеет целью нарушение функционирования физических каналов распространения информации в информационной инфраструктуре противоборствующей стороны и вскрытие ее системы криптографической защиты. В рамках электронного подавления различают технические и криптографические операции. Технические операции электронного подавления ориентированы на вывод из строя приемопередающих комплексов противоборствующей стороны, а криптографические операции - на вскрытие и подавление семантической составляющей передаваемой информации; д) психологическое воздействие - направлено против человеческого разума, а также компьютерной поддержки процессов принятия человеком ответственных решений. Выделяется четыре разновидности этого направления *войны информационной:* операции против населения; операции против руководящего состава войск; операции против живой силы противоборствующей стороны; операции по модификации культуры; е) хакерская война - имеет целью проникновение в телекомму-

никационные и информационные системы противоборствующей стороны и нанесение ущерба этим системам и находящимся в них информационным ресурсам. Война в области экономической информации - ориентирована на нанесение ущерба экономике противоборствующей стороны путем осуществления экономической блокады или информационной агрессии. При этом под *агрессией информационной экономической* понимается монопольное владение значительной частью информационных ресурсов и доминирование с элементами диктата на рынке информационных услуг; ж) кибернетическая война - имеет целью нанесение ущерба информационным ресурсам противоборствующей стороны. Эта разновидность насильственных действий может быть реализована в виде: информационного терроризма, проявляющегося в виде разрозненных случаев насилия в отношении специально выбранных целей; информационных атак, направленных на изменение алгоритмов работы информационных систем при сохранении видимости нормального функционирования; демонстрации силы, направленной на внушение противоборствующей стороне требуемого представления о возможных последствиях применения против нее того или иного оружия; з) война инфраструктурная - действия, направленные на деградацию, нарушение или разрушение фундаментальной инфраструктуры противника без обязательного прямого поражения живой силы, т.е. направленные против систем управления и жизнеобеспечения государства противника - тех его элементов, активов и структур, которые обеспечивают материальные и организационные основы целевых действий противника. В современных условиях практически неотделима от *войны информационной.*

Война инфраструктурная информационная - термин, по сути, сводимый к объединению *войны инфраструктурной* и *войны информационной* и подразумевающий активные действия против *ресурса информационного* фундаментальных инфраструктур государства противника, а также психологическое воздействие на его население.

Война навигационная - действия, направленные на сокращение, изменение или лишение противника способности отслеживания географического местоположения и управления (т.е. навигации), основанного на таких способностях. Рассматриваются как часть методов *войны информационной*, относящихся к воздействию, в частности, на глобальную систему.

Война психологическая - 1) использование *пропаганды и других действий психологических*, имеющих первичную цель влияния на мнения, эмоции, отношения и поведение отдельных личностей, групп людей и население противника таким способом, чтобы поддержать достижение целей войны; 2) *действия психологические*, направленные на решение политических, военных, экономических и идеологических задач с целью создавать

в отношении враждебного государства эмоции, отношения или поведение, способствующие достижению своих целей.

Война сетевая (Война компьютерная) - принцип организации ведения военных действий, при котором силы и средства организуются не по принципу иерархического подчинения, а по принципу сети, соответственно меняется и принцип организации управления. Такой принцип традиционно используется крупными террористическими организациями. Применялся он и в партизанских движениях. Сетевой принцип используется хакерскими группами. Многие аналитики считают его основным в *войне информационной.*

Война систем информационная - подкатегория *войны информационной*. *Война систем информационная* нацелена на системы обработки информации, каналы и средства передачи информации, прекращение или нарушение деятельности которых обеспечивает тактическое и стратегическое преимущество.

Вооруженный конфликт - вооруженное столкновение ограниченного масштаба между государствами (международный вооруженный конфликт) или противостоящими сторонами в пределах территории одного государства (внутренний вооруженный конфликт);

Вооруженный конфликт - вооруженное столкновение ограниченного масштаба между государствами (международный вооруженный конфликт) или противостоящими сторонами в пределах территории одного государства (внутренний вооруженный конфликт);

Глобализация - процесс распространения информационных технологий, продуктов и систем по ' всему миру, несущий за собой экономическую и культурную интеграцию. Сторонники этого процесса видят в нем возможности дальнейшего прогресса при условии развития глобального информационного общества. Оппоненты предупреждают об опасностях глобализации для национальных культурных традиций.

Глобальная безопасность - вид безопасности для всего человечества, т.е. защита от опасностей всемирного масштаба, угрожающих существованию людского рода или способных привести к резкому ухудшению условий жизнедеятельности на планете. К таким угрозам прежде всего относят глобальные проблемы современности. **Важными направлениями укрепления глобальной безопасности являются**: разоружение и контроль над вооружениями; защита окружающей среды, содействие экономическому и социальному прогрессу развивающихся стран; эффективная демографическая политика, борьба с международным терроризмом и незаконным оборотом наркотиков; предотвращение и урегулирование этнополитических конфликтов; сохранение культурного многообразия в современном мире;

обеспечение соблюдения прав человека; освоение космоса и рациональное использование богатств Мирового океана и т.п.

Глобальная вычислительная сеть - сеть, покрывающая значительную географическую территорию (регион, страну, ряд стран). **Интернет** является крупнейшей глобальной вычислительной сетью.

Глобальная информационная инфраструктура - качественно новое информационное образование, формирование которого начала в 1995 г. группа развитых стран мирового сообщества. По их замыслу Г.и.и. будет представлять собой интегрированную общемировую информационную сеть массового обслуживания населения нашей планеты на основе интеграции глобальных и региональных информационно-коммуникационных систем, а также систем цифрового телевидения и радиовещания, спутниковых систем и подвижной связи.

Глобальная информационная окружающая среда - полная общемировая совокупность *пространств информационных* и *ресурсов информационных*.

Глобальная сеть связи - предназначена для оказания услуг на основной части Земного шара и находящаяся под международным регулированием.

Государственная политика в области защиты информации имеет следующие основные направления: 1) создание механизмов государственного управления деятельностью в области защиты информации; 2) развитие законодательства в сфере защиты информации; 3) защита государственных информационных ресурсов; 4) создание условий для развития рынка современных технологий и услуг по защите информации; 5) организация защиты наиболее важных для функционирования государства и общества автоматизированных информационных систем (государственных органов власти и управления, платежной системы Национального банка, управления стратегическими объектами, критичными технологическими процессами и другими критичными объектами национальной инфраструктуры); 6) реализация и поддержка программ и проектов по защите информации.

Государственная политика в области информатизации - комплекс взаимоувязанных политических, правовых, экономических, социально-культурных и организационных мероприятий, направленный на установление общегосударственных приоритетов развития информсреды общества и создания условий перехода к информобществу.

Дампстер - методика анализа уничтожаемой пользователем информации с целью определения его идентифицирующих признаков для последующего их использования в незаконных целях, в частности, для проникновения в массивы информационные или совершения иных действий от имени данного пользователя.

Данные - представление фактов, суждений (знаний) или указаний формализованным способом в виде знаков или аналоговых сигналов, подходящим для связи, интерпретации или обработки автоматизированными средствами, а также восприятием человеком в любой доступной форме.

Данные персональные - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие (способствующие) идентифицировать его личность.

Двойная конвертация - представление информации в виде содержания и конверта сообщения в новом внешнем конверте, с целью ее защиты всякий раз, когда сообщение отправлено через недостаточно надежную область информационной сети. Содержание внешнего конверта может быть зашифровано в зависимости от степени доверия к сетевому графику.

Дезинформация - 1**)** меры, направленные на введение в заблуждение противника с помощью подтасовки, искажения или фальсификации информации, вынуждающие его действовать в ущерб своим интересам; 2) заведомо ложные сведения, распространяемые или передаваемые с целью введения в заблуждение.

Дезинформация техническая - создание ложной информации об объекте защиты путем воспроизведения несуществующих или искажения действительных демаскирующих признаков.

Действия психологические - запланированные действия, направленные на доведение специально отобранной информации и индикаторов потребителю (конкретным субъектам, группам, населению) с тем, чтобы повлиять на его эмоции, поводы, цели, рассуждения и в конечном счете поведение противника (его правительства, организаций, групп и индивидуумов). Вспомогательная цель может состоять в том, чтобы стимулировать или укрепить у противника отношения и поведение, благоприятные для целей субъекта *действия психологического*. Синоним: операции психологические.

Действия психологические стратегические - *действия психологические,* проводимые с широкими или долгосрочными целями в координации с общим стратегическим планированием, с постепенными результатами, осуществимыми в будущем. Направлены на руководящие круги, командование, личный состав вооруженных сил и гражданское население противника в его тылу или прифронтовой полосе позади боевых зон или на аналогичные круги дружественных противнику или нейтральных стран.

Диверсия информационная - криминальное действие, по объективным признакам схожее с *кибертерроризмом,* однако в качестве цели имеющее подрыв экономической безопасности и обороноспособности.

Доведение сведений - вид *действия психологического*. Доведение через СМИ или по другим каналам информации до субъекта, группы или общества с целью убедить объект воздействия (индивидуума или группу) изменить или сформировать мнения, эмоции, отношения и форму поведения, а в конечном итоге предпринять конкретные поступки в заданных интересах.

Доминирование инструментальное (в противоположность *доминированию информационному* в данном контексте) подавляющее преимущество, полученное за счет превышающих технических возможностей (силы) относительно любой формы передачи данных в уместных информационных действиях.

Доступ фрикерский - проникновение в телекоммуникационную сеть для получения информации обмена кодами доступа, их изменения и использования в своих целях, взлом системы защиты.

Задняя дверь *(люк, черный ход)* - 1) дополнительная точка входа в операционной системе или другом базовом программном обеспечении компьютерной системы, позволяющая пройти в процесс обработки информации в обход средств обеспечения безопасности системы, преднамеренно встроенная проектировщиками или разработчиками программных средств; 2) скрытое программное обеспечение или механизм аппаратных средств ЭВМ, предназначенные для обхода средств безопасности.

Ивент-анализ - анализу подвергаются отобранные экспертами описания событий (документы, фрагменты документов, краткие сообщения).Событие описывается с помощью категорий, используемых в контент-анализе.

Инфократия (киберкратия) - термин, еще не достаточно определенный и распространенный. Ассоциируется со способом правления или проведением политики, в которых информация и доступ в глобальные информационные сети являются доминирующим источником полномочия. Этот термин лингвистически означает управление посредством информации. Сторонники такой концепции исходят из того, что информация и управление на ее основе станут доминирующим источником власти как естественный следующий шаг в политическом развитии общества.

Информации утечка - совершившийся факт разглашения (распространения) информации ограниченного доступа за пределами санкционированного круга лиц в результате совершенных действий неправомочных.

Информационное противоборство - борьба в информационной сфере, которая предполагает комплексное деструктивное воздействие на информацию, информационные системы и информационную инфраструктуру противоборствующей стороны с одновременной защитой собствен-

ной информации, информационных систем и информационной инфраструктуры от подобного воздействия. Конечной целью информационного противоборства является завоевание и удержание информационного превосходства над противоборствующей стороной.

Информационное противоборство - соперничество социальных систем в информационно-психологической сфере по поводу влияния на те или иные сферы социальных отношений и установления контроля над источниками стратегических ресурсов, в результате которого одни участники соперничества получают преимущества, необходимые им для дальнейшего развития, а другие их утрачивают.

Информационной безопасности угроза - факторы, создающие опасность основным интересам личности, общества и государства в информационном пространстве.

Информационно-психологическая безопасность - состояние защищенности граждан, их отдельных групп и социальных слоев, а также населения в целом от неактивных информационно-психологических воздействий.

Информационно-психологическая война - это политический конфликт по поводу власти и осуществления политического руководства, в котором политическая борьба происходит в форме информационно-психологических операций с применением информационного оружия.

Информация в войне / информация в военных средствах - термин, который обозначает применение информации и информационных технологий в контексте ведения военных действий (традиционно понимаемых), вне ассоциации с информационной войной и информационным оружием.

Информация документированная - *информация*, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать.

Информация конфиденциальная - сведения ограниченного доступа, не отнесенные к государственной тайне. К *информации конфиденциальной*, в частности, относятся сведения, составляющие служебную и коммерческую тайны, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, личную и семейную тайну, а также сведения, раскрывающие частную жизнь граждан.

Информация критическая - определенные факты относительно намерений, способностей и действий, жизненно необходимых для эффективного управления и деятельности *структур критически важных*, эффективного выполнения стоящих стратегических задач.

Информация о гражданах (персональные данные) - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Информация распорядительная - сведения, возникающие в связи с реализацией человеком некоторых нормативных предписаний, инструкций: заполнение служебных журналов, управление движением автотранспорта, производственным станом и пр.

Информация экономическая - до конца не определенный (в связи с неопределенностью термина экономика) термин, затрагивающий весьма широкий круг фактов, процессов, явлений и лиц, задействованных в деятельности объектов хозяйствования, производственных предприятий, финансовых и кредитно-денежных организаций, включая инвестиционные процессы. К *информации экономической* может быть отнесена коммерческая информация и реклама.

Инфраструктура информационная глобальная - всемирная взаимосвязь сетей связи, компьютерной техники, баз данных и бытовой электроники, делающая доступной для пользователей обширные объемы информации. Охватывает широкий спектр оборудования, включающий камеры, сканеры, клавиатуры, факсы, компьютеры, коммутаторы, компакт-диски, видео- и аудиопленки, провода, кабели, спутники, волоконно-оптические линии передач, сети всех типов, телевизоры, мониторы, принтеры и многое другое.

Искусственный интеллект, машинный интеллект - область, которая рассматривается как часть науки о компьютерах, связанная с моделированием и системами, реализующими функции, такие как рассуждение и обучение, обычно ассоциируемые с человеческим интеллектом. Область информатики, занимающаяся научными исследованиями и разработкой методов и средств для правдоподобной имитации отдельных функций человеческого интеллекта с помощью автоматизированных систем. В рамках И.и. создаются методы, программные и технические средства решения задач, для которых отсутствуют формальные алгоритмы: распознавание изображений, понимание естественных языков и речи, обучение с учетом способностей ученика, постановка диагнозов, доказательство теорем и т. п. Эти задачи обычно решаются человеком с привлечением подсознания и поэтому их довольно трудно моделировать. На основе методов И.и. разрабатываются программные интеллектуальные системы, например, интеллектуальные информационные системы, интеллектуальные обучающие системы, интеллектуальные системы программирования и др. Большинство таких систем используют для своей работы соответствующие базы знаний, которые также разрабатываются с привлечением методов И.и. Иногда программы И.и. служат для моделирования поведения человека, а

иногда - для технических применений. Методы И.и. помогают и в программировании компьютерных игр. Термин «машинный интеллект», являясь синонимом И.и., чаще служит для указания только технологического аспекта проблемы И.и. Свойство автоматических и автоматизированных систем выполнять отдельные функции интеллекта человека, например, выбирать и принимать оптимальные решения на основе ранее полученного опыта и анализа внешних воздействий.

Кодификатор (классификатор) компьютерных преступлений - разработан в 1991 г. рабочей группой Интерпола. К.к.п. интегрирован в автоматизированную систему поиска информации по запросам и в настоящее время доступен Национальным бюро Интерпола более чем 100 стран. К.к.п. содержит шесть групп компьютерных преступлений, каждая из которых разбита на отдельные виды. В К.к.п. предусмотрена опция Z, обозначающая «прочие виды преступлений» и предназначенная для учета возможного развития компьютерных технологий.

Группа	Вид деятельности
QA – несанкционированный доступ и перехват	
QAH	Компьютерный абордаж (хакинг): несанкционированный доступ в компьютер или компьютерную сеть;
QAI	Перехват: несанкционированный перехват информации при помощи технических средств, несанкционированный обращения в компьютерную систему или сеть как из нее, так и внутри компьютерной системы или сети;
QAT	Кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты;
QAZ	Прочие виды несанкционированного доступа и перехвата.
Группа QD – изменение компьютерных данных	
QDL	Логическая бомба: неправомерное изменение компьютерных данных путем внедрения логической бомбы;
QDT	Троянский конь: неправомерное изменение компьютерных данных путем внедрения троянского коня;
QDV	Вирус: изменение компьютерных данных или программ без права на то, путем внедрения или распространения компьютерного вируса;
QDW	Червь: несанкционированное изменение компьютерных данных или программ путем передачи, внедрения или распространения компьютерного червя в компьютерную сеть;
QDZ	Прочие виды изменения данных.
Группа QF – компьютерное мошенничество	
QFC	Компьютерные мошенничества с банкоматами: мошенничества, связанные с хищением наличных денег из банкоматов;
QFF	Компьютерные подделки: мошенничества и хищения из компьютерных систем путем создания поддельных устройств (карточек и пр.);
QFG	Мошенничества с игровыми автоматами: мошенничества и хищения, связанные с игровыми автоматами;
QFM	Манипуляции с программами ввода-вывода: мошенничества и хищения

Группа	Вид деятельности
	посредством неверного ввода или вывода в компьютерные системы или из них путем манипуляции программами;
QFP	Компьютерные мошенничества с платежными средствами: мошенничества и хищения, связанные с платежными средствами;
QFT	Телефонное мошенничество: доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы;
QFZ	Прочие компьютерные мошенничества.
Группа QR – незаконное копирование	
QRG/QFS	Незаконное копирование, распространение или опубликование компьютерных игр и другого программного обеспечения;
QRT	Незаконное копирование топологии полупроводниковых изделий: незаконное копирование защищенной законом топологии полупроводниковых изделий или незаконная коммерческая эксплуатация или импорт с этой целью топологии или самого полупроводникового изделия, произведенного с использованием данной топологии;
QRZ	Прочее незаконное копирование.
Группа QS – компьютерный саботаж	
QSH	Саботаж с использованием аппаратного обеспечения: ввод, изменение, стирание или подавление компьютерных данных или программ или вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы;
QSS	Компьютерный саботаж программы: несанкционированное стирание, повреждение, ухудшение или подавление компьютерных данных или программ;
QSZ	Прочие виды саботажа.
Группа QZ – прочие компьютерные преступления	
QZB	Электронные доски объявлений (BBS): использование BBS для хранения, обмена и распространения материалов, имеющих отношение к преступной деятельности;
QZE	Хищение информации, представляющей коммерческую тайну (компьютерный шпионаж): приобретение незаконными средствами или передача информации, представляющей коммерческую тайну без права на то или другого законного обоснования, с намерением причинить экономический ущерб или получить незаконные экономические преимущества;
QZS	Материал конфиденциального характера: использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера;
QZZ	Прочие компьютерные преступления.

Коннект-анализ - анализу подвергаются явные и латентные контакты субъектов межгосударственных отношений, персон и т.д.

Контент-анализ - метод для регулярного и целенаправленного изучения информисточников (продукция СМИ, книги, аудио- и видеозаписи, пра-

вительственные и дипломатические документы, тексты речей, письма, дневники и т.д.) на основе определенных тем и специально разработанных форм, использующийся с целью оперативного реагирования на полученные в ходе исследования результаты.

Конфликт - реальная борьба между странами, людьми или группами, независимо от того, каковы истоки этой борьбы, ее способы и средства, мобилизуемые каждой из сторон.

Фаза конфликта	Этап конфликта	Возможности разрешения конфликта (%)
Начальная фаза	Возникновение и развитие конфликтной ситуации; осознание конфликтной ситуации	**92%**
Эскалация	Начало открытого конфликтного взаимодействия	**46%**
Пик конфликта	Развитие открытого конфликта	**Менее 5%**
Фаза спада	-	**Около 20%**

Кризис - суд, перелом, переворот, пора переходного состояния, перелом, при котором неадекватность средств достижения целей рождает непредсказуемые проблемы. *Кризис* проявляет скрытые конфликты и диспропорции. Яркий пример кризиса - революция.

Крупномасштабная война - война между коалициями государств или крупнейшими государствами мирового сообщества, в которой стороны будут преследовать радикальные военно-политические цели. *Крупномасштабная война* может стать результатом эскалации вооруженного конфликта, локальной или региональной войны с вовлечением значительного количества государств разных регионов мира. Она потребует мобилизации всех имеющихся материальных ресурсов и духовных сил государств-участников;

Локальная война - война между двумя и более государствами, преследующая ограниченные военно-политические цели, в которой военные действия ведутся в границах противоборствующих государств и которая затрагивает преимущественно интересы только этих государств (территориальные, экономические, политические и другие);

Локальная война - война между двумя и более государствами, преследующая ограниченные военно-политические цели, в которой военные действия ведутся в границах противоборствующих государств и которая затрагивает преимущественно интересы только этих государств (территориальные, экономические, политические и другие).

Международная безопасность (глобальность) - такое состояние международных отношений, при котором исключено нарушение всеобщего

мира, гарантировано устойчивое и стабильное развитие мирового сообщества в экономической, социально-политической и духовной областях, созданы условия для предотвращения конфронтации, военных конфликтов и войн между государствами.

Международные отношения - совокупность экономических, политических, правовых, идеологических, дипломатических, военных, культурных и других связей и взаимоотношений между субъектами, действующими на мировой арене; самостоятельная дисциплина в сфере политических наук (выделилась в начале XX в.), традиционно занимающаяся исследованием межгосударственных взаимодействий (интеракций) в мировом масштабе, а также национальных интересов государств.

Мировая политика (англ. world politics) - сформировавшееся в 1970-е гг. в рамках неолиберализма научное направление (его развитие связывается с авторами журнала «International Organization», а также с работой Р.Кеохейна и Дж.Ная «Транснациональные отношения и мировая политика».). Хотя понятия «международные отношения» и «мировая политика» используются часто как синонимы, в первом случае акцент делается обычно на межгосударственных проблемах, а во втором - на том, что рассматривается более широкий круг акторов (включая неправительственные) и проблем (в том числе связанных с глобализацией, а также экологических и т.д.). Таким образом, в большинстве современных исследований по данной проблематике международные отношения выступают частью мировой политики.

Модернизация - процесс быстро увеличивающегося контроля над природой с помощью тесного сотрудничества между людьми. Он включает в себя интеллектуальную (в т.ч. рационализация и секуляризация), технологическую (индустриализация, урбанизация и т.д.), социальную (дифференциация общественных групп и пр.) революции (определение принадлежит Д.Растоу).

Мягкая сила - способность государства (союза, коалиции) достичь желаемых результатов в международных делах через убеждение (притяжение), а не подавление (навязывание, принуждение). «Мягкая сила» действует, побуждая других следовать (или добиваясь их собственного согласия следовать, или делая выгодным следование) определенным нормам поведения и институтам на международной арене, что и приводит ее носителей к достижению желаемого результата фактически без принуждения» (хотя и здесь, конечно, может быть определенная вынужденность поведения, обусловленная отсутствием иной альтернативы).

Национальная безопасность - состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уро-

вень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие РФ, оборону и безопасность государства;

Национальные интересы РФ - совокупность внутренних и внешних потребностей государства в обеспечении защищенности и устойчивого развития личности, общества и государства;

Противоборство информационное: 1) форма межгосударственного противоборства, предусматривающая целенаправленное использование специально разработанных средств для воздействия на ресурс информационный противостоящей стороны и защиты собственных ресурсов в интересах достижения поставленных политических и военных целей; 2)форма межгосударственного соперничества, реализуемая посредством познания воздействия информационного на системы правления других государств и их вооруженных сил, а та же на политическое и военное руководство и общество в целом, инфраструктуру информационную и СМИ этих государств для достижения выгодных себе целей при одновременной защите от аналогичных действий своего пространства информационного. («Информационная глобализация и Россия: вызовы и возможности»)

Региональная безопасность - составная часть международной безопасности, характеризующая состояние международных отношений в конкретном регионе мирового сообщества как свободное от военных угроз, экономических опасностей и т.п., а также от вторжений и вмешательств извне, связанных с нанесением ущерба, посягательств на суверенитет и независимость государств региона.

Региональная война - война с участием двух и более государств одного региона, ведущаяся национальными или коалиционными вооруженными силами с применением как обычных, так и ядерных средств поражения, на территории региона с прилегающими к нему акваториями и в воздушном (космическом) пространстве над ним, в ходе которой стороны будут преследовать важные военно-политические цели;

Силы обеспечения нацбезопасности - Вооруженные Силы РФ, другие войска, воинские формирования и органы, в которых федеральным законодательством предусмотрена военная и (или) правоохранительная служба, а также федеральные органы госвласти, принимающие участие в обеспечении нацбезопасности государства на основании законодательства РФ.

Система обеспечения нацбезопасности - силы и средства обеспечения нацбезопасности.

Средства обеспечения нацбезопасности - технологии, а также технические, программные, лингвистические, правовые, организационные средства, включая телекоммуникационные каналы, используемые в системе

обеспечения нацбезопасности для сбора, формирования, обработки, передачи или приема информации о состоянии нацбезопасности и мерах по ее укреплению.

Стратегические национальные приоритеты - важнейшие направления обеспечения нацбезопасности, по которым реализуются конституционные права и свободы граждан РФ, осуществляются устойчивое социально-экономическое развитие и охрана суверенитета страны, ее независимости и территориальной целостности.

Угроза национальной безопасности - прямая или косвенная возможность нанесения ущерба конституционным правам, свободам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию РФ, обороне и безопасности государства.

ПРИЛОЖЕНИЯ

Утверждена
распоряжением Президента
Российской Федерации
от 17 декабря 2009 г. N 861-рп

КЛИМАТИЧЕСКАЯ ДОКТРИНА РОССИЙСКОЙ ФЕДЕРАЦИИ

Изменение климата является одной из важнейших международных проблем XXI века, которая выходит за рамки научной проблемы и представляет собой комплексную междисциплинарную проблему, охватывающую экологические, экономические и социальные аспекты устойчивого развития Российской Федерации.

Особенную обеспокоенность вызывает беспрецедентно высокая скорость глобального потепления, наблюдаемая в течение последних десятилетий. Современная наука предоставляет все более веские основания в подтверждение того, что хозяйственная деятельность человека, связанная прежде всего с выбросами парниковых газов в результате сжигания ископаемого топлива, оказывает заметное влияние на климат.

Изменения климата многообразны и проявляются, в частности, в изменении частоты и интенсивности климатических аномалий и экстремальных погодных явлений. В течение XXI века высока вероятность ускорения динамики наблюдаемых изменений климата.

Ожидаемые изменения климата неизбежно отразятся на жизни людей, на состоянии животного и растительного мира во всех регионах планеты, а в некоторых из них станут ощутимой угрозой для благополучия населения и устойчивого развития.

Указанные факторы предопределяют необходимость учета изменений климата в качестве одного из ключевых долговременных факторов безопасности Российской Федерации и выдвигают проблему глобального изменения климата в ее национальном и международном измерениях в число приоритетов политики Российской Федерации.

Последствия изменений климата проявляются на глобальном, региональном, субрегиональном и национальном уровнях.

Глобальное изменение климата создает для Российской Федерации (с учетом размеров ее территории, географического положения, исключительного разнообразия климатических условий, структуры экономики, демографических проблем и геополитических интересов) ситуацию, которая предполагает необходимость заблаговременного формирования всеобъемлющего и взвешенного подхода государства к проблемам климата и смежным вопросам на основе комплексного научного анализа экологических, экономических и социальных факторов.

I. Общие положения

1. Настоящая Доктрина представляет собой систему взглядов на цель, принципы, содержание и пути реализации единой государственной политики Российской Федерации внутри страны и на международной арене по вопросам, связанным с изменением климата и его последствиями (далее - политика в области климата).

Учитывая стратегические ориентиры Российской Федерации, настоящая Доктрина является основой формирования и реализации политики в области климата.

2. Правовую основу настоящей Доктрины составляют Конституция Российской Федерации, федеральные законы, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, Рамочная конвенция Организации Объединенных Наций об изменении климата от 9 мая 1992 г. и другие международные договоры Российской Федерации, в том числе по проблемам окружающей среды и устойчивого развития.

3. Настоящая Доктрина базируется на фундаментальных и прикладных научных знаниях в области климата и в смежных областях, включая:

оценку прошлого и современного состояния климатической системы;

оценку факторов влияния антропогенной деятельности на климат;

прогноз возможных изменений климата и их влияние на качество жизни населения Российской Федерации и других регионов Земли;

оценку степени защищенности и уязвимости экологических систем, экономики, населения, государственных институтов и инфраструктуры государства по отношению к изменениям климата и существующих возможностей адаптации к ним;

оценку возможностей смягчения антропогенного воздействия на климат.

4. В основу настоящей Доктрины положен анализ результатов проводимых на территории Российской Федерации и в других регионах Земли исследований климатических изменений и последствий влияния этих изменений на различные сектора экономики, население и окружающую среду с учетом результатов работ, связанных с практическим использованием климатической информации органами государственной власти. Научное обоснование настоящей Доктрины включает признание способности антропогенного фактора оказывать воздействия на климатическую систему, приводящие к значимым, в первую очередь неблагоприятным и опасным для человека и окружающей среды, последствиям. Особенностью реакции климата как на антропогенное воздействие, так и на меры по смягчению антропогенного воздействия является ее запаздывание по отношению к такому воздействию. В рамках политики в области климата эта особенность предопределяет важную роль своевременной адаптации к неизбежным в ближайшие десятилетия климатическим изменениям.

5. Настоящая Доктрина как политический документ признает, что проблемы, связанные с изменениями климата, в частности обеспечение баланса между эффективностью экономики и социальной справедливостью, устранение потенциальных конфликтов интересов в связи с экстремальными проявлениями изменений климата (тепловые волны, наводнения, засухи и другие явления), не могут быть решены при помощи только научных методов. В подобных ситуациях поиск баланса является предметом политического выбора.

II. Цель и принципы политики в области климата

6. Стратегической целью политики в области климата является обеспечение безопасного и устойчивого развития Российской Федерации, включая институциональный, экономический, экологический и социальный, в том числе демографический, аспекты развития в условиях изменяющегося климата и возникновения соответствующих угроз.

7. Основными принципами политики в области климата являются:

глобальный характер интересов Российской Федерации в отношении изменений климата и их последствий;

приоритет национальных интересов при разработке и реализации политики в области климата;

ясность и информационная открытость политики в области климата;

признание необходимости действий как внутри страны, так и в рамках полноправного международного партнерства Российской Федерации в международных исследовательских программах и проектах, касающихся изменений климата;

всесторонность учета возможных потерь и выгод, связанных с изменениями климата;

предосторожность при планировании и реализации мер по обеспечению защищенности человека, экономики и государства от неблагоприятных последствий изменений климата.

8. Интересы Российской Федерации, связанные с изменениями климата, не ограничиваются ее территорией и носят глобальный характер. Это обусловлено как глобальным характером изменений климата, так и необходимостью учитывать в международных отношениях многообразие воздействий на климат и последствий изменений климата в различных регионах Земли. При построении политики в области климата необходимо учитывать не только прямые, но и опосредованные, в том числе отдаленные, воздействия климатических изменений на природную среду, экономику, население и на различные его социальные группы. К опосредованным воздействиям климатических изменений относится их влияние на миграционные процессы в результате глобального перераспределения природных, в том числе продовольственных и водных, ресурсов и снижения относительной комфортности проживания человека в отдельных регионах Российской Федерации и за ее пределами.

9. Ожидаемые изменения климата являются причиной угроз безопасности Российской Федерации. В этих условиях важна самостоятельность в оценках и выводах, полученных на основе полной, объективной и достоверной информации о текущих и возможных в будущем климатических изменениях, об их последствиях для Российской Федерации и других стран и о надлежащих мерах по адаптации и смягчению отрицательных последствий этих изменений.

10. С учетом этого необходимым условием политики в области климата являются государственная поддержка и обеспечение соответствия мировому уровню:

систематических наблюдений за климатом;

фундаментальных и прикладных исследований в области климата и смежных областях науки;

применения результатов исследований для оценки рисков и выгод, связанных с последствиями изменений климата, а также возможности адаптации к этим последствиям.

11. Российская Федерация исходит из необходимости открытого обсуждения принципов формирования, содержания и механизмов реализации политики в области климата, которые выносятся на широкое общественное обсуждение, в том числе с участием институтов гражданского общества и деловых кругов, с целью принятия соответствующих решений с учетом законодательства Российской Федерации. Политические решения в отношении климата и основанные на них правовые нормы необходимо ориентировать на интересы Российской Федерации в долгосрочной перспективе, что обусловлено тенденциями изменения климатических факторов и необходимостью принятия постоянных мер по адаптации и смягчению антропогенного воздействия на климат.

12. Ясность и информационная открытость политики в области климата необходимы на всех уровнях и для всех субъектов общественных отношений, в том числе для:

федеральных органов исполнительной власти, поскольку во многих сферах государственного управления, связанных в первую очередь с развитием государственной инфраструктуры, при выработке государственной политики и нормативно-правового регулирования необходимо учитывать погодно-климатические факторы и соответствующие риски;

органов государственной власти субъектов Российской Федерации и органов местного самоуправления, поскольку при средне- и долгосрочном планировании социально-экономического развития территорий необходимо учитывать изменения климата и возможность адаптации к ним;

национального и международного бизнес-сообществ, поскольку их инвестиционная активность зависит от возможности уверенно рассчитывать инвестиционные риски, связанные с изменениями климата, и от возможности управления этими рисками;

населения, поскольку, с одной стороны, изменения климата сказываются на социальных факторах (изменение условий комфортного проживания и предпочтений населения при выборе места жительства, изменения на рынке труда и другие факторы), а с другой - поведенческие факторы населения существенным образом

влияют на потенциал осуществимости и эффективность мер по адаптации и смягчению антропогенного влияния на климат.

13. Несмотря на обширные и убедительные научные данные о происходящих и прогнозируемых климатических изменениях, сохраняется значительная неопределенность в оценках того, как именно будут протекать климатические изменения и какое они окажут влияние на экологические системы, экономическую и политическую деятельность, а также на социальные процессы в разных странах и регионах. Российская Федерация исходит из необходимости действий в условиях неопределенности оценок будущих изменений климата и их последствий и готова к ответственному и конструктивному участию в соответствующих международных инициативах. Действия должны основываться на научно обоснованной оценке рисков, необходимости заблаговременного принятия мер по их уменьшению или предотвращению, повышению защищенности жизненно важных интересов личности, общества и государства от воздействия изменений климата. При этом снижение существующего уровня неопределенности оценок будущих изменений климата и их последствий для Российской Федерации остается неизменным приоритетом климатических исследований, поддерживаемых государством.

14. Последствия изменений климата различны для регионов Российской Федерации, а в пределах одного региона по-разному влияют на группы населения, отрасли экономики и природные объекты. В связи с этим однозначная оценка последствий вероятных изменений климата для Российской Федерации невозможна и при выработке политики в области климата следует учитывать весь комплекс потерь и выгод, связанных с изменениями климата.

15. Население, природные объекты, объекты экономики, военные объекты и объекты государственной инфраструктуры различаются по характеру и степени их уязвимости к неблагоприятным последствиям изменений климата. При этом не все виды возможного ущерба могут быть оценены в денежном выражении, а сами оценки возможных потерь могут быть неопределенными. Это не должно становиться препятствием для обеспечения приемлемого уровня защищенности как меры разумной предосторожности для наиболее уязвимых территорий, объектов и социальных групп, а должно стать предметом особого внимания при оценке их уязвимости, разработке и реализации заблаговременных мер по предотвращению и нейтрализации

неблагоприятных последствий изменения климата либо их сведению к минимально возможному уровню.

16. Политика в области климата подлежит регулярной и своевременной корректировке с учетом новых знаний о климате, включая уточнение оценок его возможных изменений, экономического и технологического развития, особенно в сфере производства, передачи и потребления энергии и энергоресурсов, а также с учетом изменений политики других стран и мирового сообщества в целом, динамики международного взаимодействия в области климата и предлагаемых на международном уровне мер.

III. Содержание политики в области климата

17. Содержание политики в области климата определяется задачами, которые подчинены достижению ее стратегической цели и решаются с учетом особенностей Российской Федерации в контексте проблемы изменений климата.

18. Основными задачами политики в области климата являются:

укрепление и развитие информационной и научной основы политики в области климата, включая усиление научно-технического и технологического потенциала Российской Федерации, обеспечивающего максимальную полноту и достоверность информации о состоянии климатической системы, воздействиях на климат, его происходящих и будущих изменениях и об их последствиях;

разработка и реализация оперативных и долгосрочных мер по адаптации к изменениям климата;

разработка и реализация оперативных и долгосрочных мер по смягчению антропогенного воздействия на климат;

участие в инициативах международного сообщества в решении вопросов, связанных с изменениями климата и смежными проблемами.

19. Пополнение знаний о климатической системе является необходимой предпосылкой формирования и реализации независимой, научно и социально обоснованной политики в области климата. Систематические наблюдения за климатом, фундаментальные и прикладные исследования, связанные с его изменениями, обеспечивают повышение осведомленности органов государственной власти, субъектов экономики, научной общественности, средств массовой информации, населения о происходящих и будущих изменениях климата и об их

последствиях, о возможностях адаптации к этим изменениям и мерах по их смягчению, а также принятие соответствующих решений.

Своевременное выявление и оценка связанных с изменениями климата угроз устойчивому развитию и безопасности Российской Федерации, включая угрозы обороноспособности, экономике, состоянию окружающей среды, жизни и здоровью населения, относятся к числу приоритетов политики в области климата.

20. Адаптация к изменениям климата необходима для снижения потерь и использования выгод, связанных с наблюдаемыми и будущими изменениями климата.

Меры по адаптации к изменениям климата предусматриваются решениями органов государственной власти с учетом международных договоренностей Российской Федерации. Планирование, организация и осуществление мер по адаптации к изменениям климата, в том числе по упреждающей адаптации, проводятся в рамках государственной политики в области климата с учетом отраслевых, региональных и местных особенностей, а также долгосрочного характера этих мер, их масштабности и глубины воздействия на различные стороны жизни общества, экономики и государства.

21. Важнейшими составляющими при разработке и планировании мер по адаптации к изменениям климата являются оценки:

уязвимости к неблагоприятным последствиям изменений климата и рисков связанных с ними потерь;

возможностей получения выгод, связанных с благоприятными последствиями изменений климата;

затратности, эффективности (в том числе экономической) и практической реализуемости соответствующих мер по адаптации;

потенциала адаптации с учетом экономических, социальных и других значимых факторов для государства, секторов экономики, населения и отдельных социальных групп.

22. Упреждающая адаптация к последствиям климатических изменений относится к числу приоритетов политики в области климата.

23. Российская Федерация максимально концентрирует усилия на снижении антропогенных выбросов парниковых газов и увеличении их абсорбции поглотителями и накопителями. С этой целью предусматривается реализовать меры, обеспечивающие:

повышение энергетической эффективности во всех секторах экономики;

развитие использования возобновляемых и альтернативных источников энергии;

сокращение рыночных диспропорций, реализацию мер финансовой и налоговой политики, стимулирующих снижение антропогенных выбросов парниковых газов;

защиту и повышение качества поглотителей и накопителей парниковых газов, включая рациональное ведение лесного хозяйства, облесение и лесовозобновление на устойчивой основе.

24. Выработка предложений по обязательствам в отношении снижения выбросов парниковых газов осуществляется на основании национальных интересов при участии всех заинтересованных российских организаций.

Эффективная политика в области климата призвана стать важным фактором и катализатором динамичной технологической модернизации всей экономики страны, укрепления ее позиций в мировом экономическом сообществе, повышения конкурентоспособности в первую очередь за счет энергоэффективности.

Российская Федерация будет способствовать исследованиям и разработкам в области энергоэффективности, развития использования возобновляемых источников энергии, технологий поглощения парниковых газов и разработки инновационных экологически приемлемых технологий.

Создание и обеспечение функционирования правовых основ и механизмов государственного регулирования, направленного на сокращение антропогенного воздействия на глобальную климатическую систему, относятся к числу приоритетов политики в области климата.

25. Российская Федерация участвует в выработке коллективных мер международного сообщества по смягчению антропогенного воздействия на климат и оказывает совместно с другими членами международного сообщества содействие развивающимся странам, в том числе наиболее уязвимым по отношению к отрицательным последствиям изменений климата, в реализации мер по адаптации и смягчению негативных последствий изменений климата. При этом Российская Федерация исходит из того, что всеобъемлющее и ориентированное на долгосрочную перспективу решение климатической проблемы возможно лишь при условии обеспечения универсального характера соответствующего международного режима и участия в нем всех основных стран-эмитентов парниковых газов на основе принципов Рамочной конвенции Организации Объединенных Наций об изменении

климата, в том числе принципа общей, но дифференцированной ответственности, подразумевающего справедливую нагрузку на страны с учетом их уровня социально-экономического развития и природно-климатической специфики.

IV. Особенности Российской Федерации при решении проблемы изменений климата

26. Значительная часть территории Российской Федерации находится в области максимальных (как наблюдаемых, так и прогнозируемых) изменений климата.

Происходящие и ожидаемые изменения климата, в первую очередь негативные, и последствия этих изменений оказывают существенное воздействие на социально-экономическое развитие страны в целом, на жизнь и здоровье ее граждан.

27. К отрицательным последствиям ожидаемых изменений климата для Российской Федерации относятся:

повышение риска для здоровья (увеличение уровня заболеваемости и смертности) некоторых социальных групп населения;

рост повторяемости, интенсивности и продолжительности засух в одних регионах, экстремальных осадков, наводнений, опасного для сельского хозяйства переувлажнения почвы - в других;

повышение пожароопасности в лесных массивах;

деградация вечной мерзлоты в северных регионах с ущербом для строений и коммуникаций;

нарушение экологического равновесия, в том числе вытеснение одних биологических видов другими;

распространение инфекционных и паразитарных заболеваний;

увеличение расходов электроэнергии на кондиционирование воздуха в летний сезон для значительной части населенных пунктов.

28. К возможным положительным для Российской Федерации последствиям ожидаемых изменений климата, с которыми связан значительный потенциал эффективного отраслевого и регионального экономического развития, относятся:

сокращение расходов энергии в отопительный период;

улучшение ледовой обстановки и, соответственно, условий транспортировки грузов в арктических морях, облегчение доступа к арктическим шельфам и их освоения;

улучшение структуры и расширение зоны растениеводства, а также повышение эффективности животноводства (при выполнении ряда дополнительных условий и принятии определенных мер);

повышение продуктивности бореальных лесов.

29. По сравнению со многими странами и регионами Земли преимуществом Российской Федерации является более высокий адаптационный потенциал страны в целом, который обеспечивают:

большие размеры территории;

наличие значительных водных ресурсов;

относительно небольшая доля населения, проживающего на территориях, особо уязвимых к изменениям климата.

30. Исключительное (по сравнению с другими странами) разнообразие и масштабы изменений климата регионов Российской Федерации и их последствий для окружающей среды, экономики и населения являются естественным следствием значительных размеров территории и многообразия природных условий.

При формировании политики в области климата, включая позиционирование Российской Федерации в мировом сообществе, необходимо учитывать сочетание низкой средней плотности населения со значительными размерами территории, приводящее к повышенным транспортным потребностям (как непосредственно для населения, так и для инфраструктуры, обеспечивающей потребности государства, населения и экономики), а также холодный климат, обусловливающий дополнительные потребности в отоплении зданий, производство и транспортировку значительных объемов топливно-энергетических ресурсов.

V. Реализация политики в области климата

31. Основными направлениями политики в области климата являются:

развитие нормативно-правовой базы и организация государственного регулирования в области изменений климата;

развитие экономических механизмов, связанных с реализацией мер по адаптации и смягчению антропогенного воздействия на климат;

научное, информационное и кадровое обеспечение разработки и реализации мер по адаптации и смягчению антропогенного воздействия на климат;

международное сотрудничество в области разработки и реализации мер по адаптации и смягчению антропогенного воздействия на климат.

32. Развитие нормативно-правовой базы в области изменений климата является основной предпосылкой создания и эффективного функционирования механизма реализации политики в этой области. Организация работы федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации по реализации конкретных мер, направленных на предотвращение и преодоление угроз национальным интересам в области изменений климата, требует дальнейшего совершенствования законодательства Российской Федерации в указанной области и обеспечения строгого его соблюдения всеми хозяйствующими субъектами. При этом необходима гармонизация законодательства Российской Федерации, регулирующего вопросы изменений климата, с соответствующими нормами международного права в рамках международных обязательств Российской Федерации. Основные принципы политики в области климата находят развитие и в законодательстве субъектов Российской Федерации.

33. Эффективность реализации мер по адаптации и смягчению антропогенного воздействия на климат существенным образом зависит от различных экономических факторов и их финансового регулирования.

Выбор экономических инструментов, способствующих снижению антропогенных выбросов парниковых газов (включая возможное использование рыночных механизмов, в том числе торговлю выбросами), будет определяться с учетом их эффективности с использованием механизмов государственного и частного финансирования.

При создании и совершенствовании национальных экономических и финансовых механизмов и их встраивании в соответствующие международные механизмы приоритетом является обеспечение защищенности жизненно важных интересов личности, общества и государства от неблагоприятных воздействий изменений климата.

Основной задачей научного обеспечения разработки и реализации политики в области климата является обеспечение государства, бизнеса и граждан страны достоверной и объективной научной информацией для принятия соответствующих решений.

34. К приоритетным направлениям научного обеспечения разработки мер по адаптации и смягчению антропогенного воздействия на климат относятся:

развитие и поддержание на территории Российской Федерации систем наблюдения за климатом, включая факторы, формирующие климат, и индикаторы изменений климата;

разработка системы критериев, параметров (пороговых значений), условий безопасности Российской Федерации и ее отдельных регионов в отношении изменений климата;

исследование и оценка возможных в будущем изменений глобального и регионального климата, а также их последствий;

разработка мер по адаптации экономики и общества к изменениям климата;

развитие методов инвентаризации источников и стоков парниковых газов;

разработка мер по смягчению антропогенного воздействия на климат прежде всего в сфере производства и потребления энергии, включая организацию исследований и разработку механизмов реализации соответствующих инновационных проектов, а также оценка экономического, социального и экологического эффекта от реализации этих мер;

независимая (в том числе международная) экспертиза результатов научных исследований в области климата и смежных областях.

35. Научное обеспечение реализации мер по адаптации и смягчению антропогенного воздействия на климат включает:

позиционирование российской климатической науки и ее интеграцию в международные программы климатических и связанных с ними исследований с учетом интересов Российской Федерации и использованием всех возможных преимуществ международного сотрудничества;

активное участие российских ученых в подготовке международных оценочных докладов об изменениях климата и других специализированных международных докладов по взаимосвязанным проблемам;

организацию регулярной подготовки национальных оценочных докладов о наблюдаемых и вероятных изменениях климата, их последствиях, возможностях адаптации и смягчения антропогенного воздействия на климат, включая оценку объемов выбросов парниковых газов в атмосферу как в настоящем, так и в будущем, а также потенциала сокращения этих выбросов;

обеспечение соответствия климатических исследований Российской Федерации мировому уровню, признания результатов российских исследований международным научным сообществом, использования их в качестве аргументов в межгосударственном политическом диалоге по проблемам климата;

разработку и реализацию государственной программы высокотехнологичного оснащения национальных центров климатических исследований.

36. Основной задачей кадрового обеспечения разработки и реализации мер по адаптации и смягчению антропогенного воздействия на климат является обеспечение исследований и разработок в области климата и смежных областях, соответствующих мировому уровню. Решение этой задачи осуществляется путем подготовки и повышения квалификации специалистов в области климата, его влияния на экономику и социальную сферу, здоровье населения и состояние окружающей среды, а также разработки и реализации инженерных и организационных мер по адаптации и смягчению антропогенного воздействия на климат, включая:

подготовку научных кадров высшей квалификации;

обучение студентов старших курсов высших учебных заведений на базе ведущих научных организаций страны;

стажировку наиболее одаренных молодых ученых и специалистов, аспирантов и студентов старших курсов в ведущих мировых научных центрах;

подготовку дипломатических кадров, а также групп профессиональных консультантов для ведения международных переговоров и подготовки международных соглашений в области климата.

37. Осведомленность всех заинтересованных сторон, в частности высших должностных лиц, федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, деловых кругов, институтов гражданского общества и населения, по вопросам изменений климата и их влияния на жизнь человека и общества и окружающую среду является одним из важнейших факторов успешного формирования и эффективной реализации политики в области климата в интересах нынешнего и будущих поколений. Приоритетными направлениями такой политики являются объективное информационное освещение проблем, связанных с изменениями климата и их последствиями, включая популяризацию научных знаний в этой области, в том числе с помощью средств массовой информации, а также воспитание у населения Российской Федерации экологической культуры.

38. Международное сотрудничество в решении глобальных и региональных проблем, связанных с изменениями климата и антропогенными воздействиями на климат, осуществляется в целях

выработки эффективных решений по проблемам климата, оптимально учитывающих глобальные факторы и национальные интересы. Формой международного сотрудничества Российской Федерации является ее участие в разработке и выполнении международных соглашений по проблемам климата, а также в деятельности международных организаций, входящих в Организацию Объединенных Наций, занимающихся проблемами климата и смежными проблемами.

Международные программы и проекты, связанные с изменениями климата и реализуемые на территории Российской Федерации, осуществляются в рамках законодательства Российской Федерации и с учетом интересов ее безопасности.

VI. Субъекты реализации политики в области климата

39. Субъектами реализации политики в области климата являются:

федеральные органы государственной власти;

органы государственной власти субъектов Российской Федерации и органы местного самоуправления;

организации, включая общественные организации (объединения);

средства массовой информации;

домашние хозяйства.

40. Возможные в будущем климатические изменения затрагивают сферы ответственности практически всех федеральных органов государственный власти. Задачами федеральных органов государственной власти в рамках выработки и реализации политики в области климата являются:

определение максимально широкого круга проблем, связанных с влиянием климатических изменений на политику, экономику, социальную сферу и окружающую среду, и выделение приоритетных направлений;

интеграция и координация работы федеральных органов государственной власти в области климата в соответствии с установленными полномочиями;

включение мер по адаптации и смягчению антропогенного воздействия на климат в среднесрочные и долгосрочные планы социально-экономического развития Российской Федерации;

создание механизмов, обеспечивающих постоянный конструктивный диалог между научным сообществом, органами

государственной власти, ответственными за принятие решений, населением и деловыми кругами.

41. Федеральные органы государственной власти обеспечивают:

развитие и применение законодательства Российской Федерации с учетом влияния климатического фактора на соответствующие отрасли экономики и население;

разработку и применение мер по адаптации к последствиям изменения климата для экономики и общества;

развитие экономических институтов и финансовых механизмов, включая системы налогообложения и финансового стимулирования, способствующих технологическому перевооружению предприятий, замене устаревшего оборудования, внедрению технологий с потенциалом снижения выбросов парниковых газов, включая энергоэффективные и энергосберегающие технологии, технологии снижения выбросов парниковых газов предприятиями топливно-энергетического комплекса, транспорта, металлургической, химической и других отраслей промышленности, а также активизацию использования возобновляемых источников энергии;

разработку законодательного акта, регулирующего вопросы инвентаризации выбросов парниковых газов в атмосферу;

ведение системы учета (российского регистра) источников выбросов и поглощения парниковых газов (включая леса, болота и сельскохозяйственные угодья), а также данных инвентаризации (кадастра) антропогенных выбросов парниковых газов и их абсорбции поглотителями;

разработку и реализацию мер по организации и функционированию системы экологического просвещения и образования;

подготовку и публикацию на регулярной основе национального доклада об изменениях климата и его последствиях для Российской Федерации.

42. При разработке региональных и муниципальных программ устойчивого развития необходимо обеспечить решение следующих задач, связанных с изменениями климата:

развитие и применение законодательства субъектов Российской Федерации с учетом влияния климатического фактора на развитие территорий, отраслей экономики и социальной сферы;

разработка и реализация мер по адаптации к изменениям климата, включая учет фактора изменения климата в среднесрочных и долгосрочных планах социально-экономического

развития регионов и муниципальных образований, а также соответствующих секторов хозяйственной деятельности;

разработка и внедрение региональных систем эффективного реагирования на опасные погодно-климатические явления;

реализация законодательного акта, регулирующего вопросы инвентаризации выбросов в атмосферу парниковых газов;

реализация мер по смягчению антропогенного воздействия на климат, включая внедрение технологий, способствующих уменьшению выбросов парниковых газов в атмосферу, а также технологий абсорбции парниковых газов.

43. На микроэкономическом уровне решение задач по адаптации и смягчению антропогенного воздействия на климат на производстве и в сфере услуг осуществляется предприятиями, в быту - домашними хозяйствами путем:

повышения эффективности производства и потребления тепловой и электрической энергии;

повышения топливной экономичности транспортных средств;

развития энергосбережения на объектах производственного и инфраструктурного назначения, включая снижение потерь энергии и энергоносителей при транспортировке;

повышения энергоэффективности зданий и развития энергосбережения в быту;

использования погодно-климатических прогнозов для повышения энергоэффективности при реализации мер по адаптации и смягчению антропогенного воздействия на климат;

увеличения доли альтернативных (в том числе неуглеродных) источников в производстве энергии;

рационального использования лесов и сельскохозяйственных земель.

44. Учитывая возможность конфликта интересов субъектов политики в области климата, профессиональным и иным общественным организациям (объединениям) и средствам массовой информации принадлежит важная роль в предотвращении обострения таких конфликтов и возникновения социальной напряженности, недопущении коррупционного лоббирования интересов отдельных заинтересованных групп. С этой целью предусматривается осуществлять обсуждение заинтересованными сторонами путей решения проблем изменений климата и их последствий для государства, общества и экономики.

Реализация политики в области климата предполагает разработку на ее основе федеральных, региональных и отраслевых программ и планов действий.

Проект
27 мая 2010 года

СОГЛАШЕНИЕ[121] МЕЖДУ РОССИЙСКОЙ ФЕДЕРАЦИЕЙ И ЕВРОПЕЙСКИМ СОЮЗОМ О СОТРУДНИЧЕСТВЕ В СФЕРЕ КРИЗИСНОГО РЕГУЛИРОВАНИЯ

Российская Федерация, с одной стороны, и Европейский союз (ЕС), с другой стороны, далее именуемые «Стороны», согласились о нижеследующем:

СТАТЬЯ 1

1. В целях настоящего Соглашения применяются следующие термины:

- «Операция кризисного регулирования» - совокупность взаимосвязанных по целям, задачам, месту и времени действий беспристрастного военного, милицейского (полицейского) и гражданского персонала, предпринимаемых с целью стабилизации обстановки в районах потенциальных или существующих конфликтов и направленных на создание условий, способствующих разрешению конфликта, поддержание или восстановление мира и безопасности, осуществляемых по мандату ООН или ОБСЕ;

- «Ведущая Сторона» - Сторона, принимающая в каждом конкретном случае решение о проведении операции кризисного регулирования;

- «Участвующая Сторона» - Сторона, изъявившая желание принять участие в операции кризисного регулирования, проводимой под эгидой другой Стороны;- «Персонал» - специально подготовленные военные, милицейские (полицейские) и гражданские специалисты Российской Федерации и государств-членов ЕС, предназначенные для участия в операциях кризисного регулирования, проводимых Российской Федерации и государствами-членами ЕС;

[121] http://www.mid.ru/infmid.nsf/e4a549143db66e48c3256fdb00f05/8b1853150268c64dc325773b004519bc?OpenDocument

- «Приглашающая Сторона» - Сторона, принимающая в каждом конкретном случае решение о проведении операции кризисного регулирования;

- «Приглашаемая Сторона» - Сторона, изъявившая желание принять участие в операции кризисного регулирования, проводимой Приглашающей Стороной.

СТАТЬЯ 2

1. В операции кризисного регулирования, проводимой Приглашающей Стороной, может по ее приглашению принять участие Приглашаемая Сторона.

2. В случае получения от Приглашающей Стороны приглашения об участии в операции кризисного регулирования Приглашаемая Сторона предоставляет Приглашающей Стороне информацию о возможных параметрах своего участия в операции кризисного регулирования

3. Приглашающая Сторона на основе предоставленной Приглашаемой Стороной информации своевременно информирует Приглашаемую Сторону о согласии на ее участие в операции в соответствии с положениями настоящего Соглашения.

4. Конкретные технические и административные условия, на которых Приглашаемая Сторона присоединяется к операции кризисного регулирования Приглашающей Стороны, определяются перед каждой операцией в Техническом протоколе, который подписывается компетентными органами сторон.

СТАТЬЯ 3

1. Настоящее соглашение не влияет на принятие решение решения Сторонами о возможном присоединении к операции кризисного регулирования в каждом отдельном случае.

2. Каждая из сторон имеет право проводить операции кризисного регулирования в качестве Ведущей Стороны.

3. Ведущая Сторона может принять решение о приглашении третьих стран к участию в операции кризисного регулирования. Участвующая Сторона может принять приглашение Ведущей Стороны и предложить внести свой вклад в операцию. В этом случае Ведущая Сторона может принять решение о присоединении Участвующей Стороны к операции.

4. В случае принятия Ведущей Стороной решения о приглашении Участвующей Стороны к участию в операции по кризисному регулированию, после того как Участвующая Сторона выразила принципиальное согласие присоединиться к операции, она предоставит Ведущей Стороне информацию о возможностях своего участия в операции.

5. Ведущая Сторона своевременно информирует Участвующую Сторону о согласии, на основе предоставленной информации, на ее участие в операции в соответствии с положениями настоящего Соглашения.

6. Приглашаемая Сторона руководствуется документами Приглашающей Стороны, которые утверждают параметры, изменяют или продлевают мандат операции кризисного регулирования, в соответствии с положениями настоящего Соглашения, а также иных договоренностей Сторон о его выполнении.

7. Приглашаемая Сторона обеспечивает выполнение своим персоналом поставленных перед ним задач в соответствии с:

- планом проведения операции;

- любыми иными договоренностями сторон о его выполнении.

8. Персонал Участвующей Стороны применяет Правила задействования персонала Приглашающей Стороны в той мере, в какой их положения не противоречат нормам ее законодательства Приглашаемой Стороны и мандату, в соответствии с которым проводится операция. О возможных ограничениях применения упомянутых Правил Приглашаемая Сторона официально уведомляет Командующего операцией.

9. Приглашаемая Сторона имеет право в любое время, после консультаций между Сторонами, прекратить свое участие в операции как по просьбе Командующего операцией, так и по собственному решению. Приглашаемая Сторона своевременно информирует Командующего операцией о любых изменениях, касающихся ее участия в операции.

СТАТЬЯ 4

1. Статус персонала Приглашаемой Стороны определяется соглашениями о статусе сил, заключенными Приглашающей Стороной с государствами, на территории которых проводится

операция, начиная с момента его прибытия в район проведения операции.

2. Приглашаемая Сторона осуществляет юрисдикцию над своим персоналом без ущерба для соглашений о статусе сил, упомянутых в пункте 1 настоящей статьи.

3. Представитель Приглашаемой Стороны принимает участие в процедурах урегулирования любых претензий, относящихся к персоналу его Стороны, в соответствии с порядком, предусмотренным в соглашениях о статусе сил, упомянутых в пункте 1 настоящей статьи.

4. Приглашаемая Сторона урегулирует претензии, связанные с участием своего персонала в операции Приглашающей Стороны, со стороны своего персонала или в отношении него. Приглашаемая Сторона принимает в соответствии со своими законами и правилами любые меры, в том числе судебного и дисциплинарного характера, в отношении своего персонала.

5. Государства-члены ЕС заявляют об отказе от претензий к Российской Федерации в связи с участием в совместной с Российской Федерацией операции кризисного регулирования совместно с Российской Федерацией.. Указанное заявление является приложением к настоящему Соглашению.

6. Российская Сторона заявляет об отказе от претензий к любому государству-члену ЕС, участвующему в операции кризисного регулирования совместно с Российской Федерацией участвующему в совместной с ЕС операции. Указанное заявление является приложением к настоящему Соглашению.

7. Статус персонала, направляемого в штаб операции, расположенный за пределами государства, на территории которого проводится операция, определяется договоренностями между компетентными органами Приглашаемой Стороны и государства, в котором расположен Штаб.

СТАТЬЯ 5

1. Стороны защищают секретную информацию друг друга, предоставленную им в рамках операции, в соответствии с требованиями к защите секретной информации, установленными их законодательством. Для этих целей степени секретности Сторон соотносятся следующим образом:

Российская Федерация ЕС

Совершенно секретно SECRET UE

Секретно CONFIDENTIEL UE

Ограничительная пометка Российской Федерации «Для служебного пользования» соответствует степени секретности ЕС «RESTREINT UE».

2. Стороны принимают соответствующие меры для того, чтобы обеспечить защиту предоставленной им в рамках операции секретной информации друг друга на уровне, эквивалентном требуемому основными принципами и минимальными стандартами защиты секретной информации ЕС, применяемыми в ЕС, а именно, Стороны:

- не используют предоставленную им секретную информацию в иных целях, чем те, для которых эта секретная информация была предоставлена;

- не раскрывают такую информацию третьим сторонам без предварительного письменного согласия Стороны, предоставившей информацию;

- обеспечивают, чтобы доступ к предоставленной им секретной информации разрешался только лицам, которым ознакомление с этой информацией необходимо в целях выполнения их официальных функций и - в отношении информации, имеющей степень секретности CONFIDENTIEL UE и выше, - которым оформлен допуск;

- обеспечивают, чтобы до предоставления доступа к секретной информации все лица, которым необходим доступ к такой информации, инструктировались и отвечали требованиям правил по защите информации той степени секретности, какую имеет информация, к которой им должен быть предоставлен доступ;

- обеспечивают, чтобы все помещения, участки, здания, рабочие кабинеты, комнаты, коммуникационные и информационные системы, в которых секретная информация или документы хранятся и/или обрабатываются, были защищены соответствующими средствами физической защиты;

- обеспечивают регистрацию предоставляемой им секретной информации по ее получении в специальном реестре;

- информируют Сторону, предоставившую информацию, обо всех случаях состоявшегося или предполагаемого разглашения или раскрытия предоставленной ей секретной информации. В таком случае Сторона, получившая информацию, начинает расследование

и принимает соответствующие меры для предотвращения повторения таких ситуаций.

3. С учетом степени секретности секретная информация передается по дипломатическим каналам, защищенными почтовыми службами либо курьером.

4. В случае заключения между Российской Федерацией и ЕС с соглашения Соглашением между Российской Федерацией и Европейским союзом о защите секретной информации, в контексте совместной операции России и ЕС применяются положения этого соглашения.

СТАТЬЯ 6

1. Командующий операцией назначается Приглашающей Стороной.

2. Персонал Приглашаемой Стороны остается под ее полным командованием.

3. Приглашаемая Сторона делегирует Командующему операцией право постановки задач своему персоналу для выполнения целей операции, начиная с момента прибытия своего персонала в район проведения операции. При планировании решений, которые могут затрагивать персонал Приглашаемой Стороны, обеспечивается полное согласование таких решений со старшими представителями персонала Приглашаемой Стороны. Приглашаемая Сторона имеет те же права и обязанности применительно к каждодневному руководству операцией, что и Приглашающая Сторона.

4. Приглашаемая Сторона назначает старших представителей, которые представляют ее персонал в штабе операции и в штабе расположения сил операции. Старшие представители могут иметь помощников. Старшие представители консультируются с руководством штабов операции по всем вопросам, касающимся проведения операции.

5. За поддержание дисциплины персонала Приглашаемой Стороны отвечает ее руководитель персонала.

СТАТЬЯ 7

1. Приглашаемая Сторона несет все расходы, связанные с участием в операции, кроме расходов, которые подлежат финансированию из общих средств.

2. Тыловое обеспечение персоналу Приглашаемой Стороны предоставляется Приглашающей Стороной на общих со всеми государствами-участниками операции условиями, если не будут достигнуты иные договоренности.

3. В случае смерти, причинения вреда здоровью, нанесения иного ущерба физическим или юридическим лицам государства или государств, на территории которых проводится операция, выплата компенсации регулируется положениями соглашений о статусе сил, указанных в пункте 1 статьи 4 настоящего Соглашения.

5. Административное управление расходами осуществляется в рамках механизма ЕС по управлению общими расходами и национальными расходами в рамках операции.

6. В случае несоблюдения любой из Сторон своих обязательств, предусмотренных в статьях 1-6 настоящего Соглашения, другая Сторона имеет право прекратить действие настоящего Соглашения, направив соответствующее уведомление за один месяц до прекращения его действия.

СТАТЬЯ 8

1. Споры между Сторонами, связанные с толкованием или применением настоящего Соглашения, разрешаются путем консультаций и переговоров.

2. Любые разногласия между Сторонами по финансовым вопросам, которые не были урегулированы в соответствии с пунктом 1 настоящей статьи, могут быть переданы согласованному между Сторонами посреднику. Любые такие разногласия, которые не удалось разрешить с помощью посредника, могут быть переданы по просьбе любой из Сторон на рассмотрение арбитража. Каждая Сторона назначает в арбитраж по одному арбитру. Назначенные таким образом арбитры избирают третьего арбитра, который будет являться Председателем арбитража. Если в течение двух месяцев со дня получения уведомления одной Стороны о передаче спора в арбитраж другая Сторона не назначит арбитра, либо если в течение двух месяцев после назначения арбитры обеих Сторон не придут к соглашению относительно третьего арбитра, любая из Сторон

может обратиться к Председателю Международного суда с просьбой произвести назначение недостающего арбитра. Если Председатель Международного суда является гражданином Российской Федерации или любого государства-члена ЕС или если он по какой-либо причине не может выполнять эту функцию, необходимые назначения производит следующий за ним по старшинству член Международного суда, который не является гражданином ни Российской Федерации, ни любого государства-члена ЕС. Арбитраж выносит решение по справедливости. Арбитры не вправе выносить решение об уплате штрафов.

Арбитры согласовывают процедуру рассмотрения спора. Местом нахождения арбитража определяется г.Брюссель (Бельгия), при рассмотрении спора используется английский язык. Решение арбитража должно содержать указание на основания, на которых оно вынесено, и принимается Сторонами в качестве окончательного решения об урегулировании спора. Каждая Сторона несет собственные расходы на проведение арбитража, а общие расходы Сторон распределяются между ними в равных долях.

СТАТЬЯ 9

1. Настоящее Соглашение вступает в силу в первый день первого месяца после того, как Стороны уведомят друг друга о завершении всех необходимых внутренних процедур.

2. Соглашение может быть изменено при обоюдном согласии Сторон.

3. Настоящее Соглашение заключено на первоначальный период в десять лет, по истечении которого Соглашение автоматически продлевается из года в год до тех пор, пока одна из Сторон не направит другой Стороне, не менее чем за шесть месяцев до истечения его срока действия, письменного уведомления о намерении прекратить действие настоящего Соглашения.

Совершено в двух экземплярах, каждый на русском и английском языках, причем оба текста имеют одинаковую силу.

Заявление государств–членов ЕС:

«Государство-член ЕС будет принимать меры к тому, чтобы по возможности при проведении операций кризисного регулирования с участием российского персонала, насколько это позволяет его законодательство, отказываться, от предъявления претензий к Российской Федерации в связи с нанесением вреда здоровью и

смертью своего персонала или ущербом или утратой какого-либо имущества, находящегося в его собственности и используемого им, если такие вред здоровью, смерть, ущерб или утрата:

– были причинены персоналом из Российской Федерации при выполнении им своих обязанностей в связи с операцией, за исключением случаев грубой неосторожности или умышленного неправомерного поведения, или

– явились следствием использования какого-либо имущества, находящегося в собственности Российской Федерации, если это имущество было использовано в связи с операцией, за исключением случаев грубой неосторожности или умышленного неправомерного поведения участвующего в операции персонала из Российской Федерации, использующего это имущество».

Заявление Российской Федерации:

«Российская Федерация будет принимать меры к тому, чтобы, по возможности при проведении операций кризисного регулирования с участием персонала государств-членов ЕС, насколько это позволяет ее законодательство, отказываться от предъявления претензий к государствам-членам ЕС в связи с нанесением вреда и смертью своего персонала или ущербом или утратой какого-либо имущества, находящегося в ее собственности и используемого ей, если такие вред здоровью, смерть, ущерб или утрата:

- были причинены персоналом из государств-членов ЕС при выполнении им своих обязанностей в связи с операцией, за исключением случаев грубой неосторожности или умышленного неправомерного поведения, или

- явились следствием использования какого-либо имущества, находящегося в собственности государств-членов ЕС, если это имущество было использовано в связи с операцией, за исключением случаев грубой неосторожности или умышленного неправомерного поведения участвующего в операции персонала из государств-членов ЕС, использующего это имущество».

Генеральная ассамблея ООН
Шестьдесят пятая сессия
Пункт повестки дня 99(y)

Меры по обеспечению транспарентности и укреплению доверия в космической деятельности

Генеральная Ассамблея,

ссылаясь на свои резолюции 60/66 от 8 декабря 2005 года, 61/75 от 6 декабря 2006 года, 62/43 от 5 декабря 2007 года, 63/68 от 2 декабря 2008 года и 64/49 от 2 декабря 2009 года,

вновь подтверждая, что предотвращение гонки вооружений в космическом пространстве устранило бы серьезную угрозу для международного мира и безопасности,

сознавая необходимость изучения дальнейших мер при выработке соглашений в целях предотвращения гонки вооружений в космическом пространстве, включая вывод оружия в космическое пространство,

ссылаясь в связи с этим на свои предыдущие резолюции, включая резолюции 45/55 B от 4 декабря 1990 года и 48/74 B от 16 декабря 1993 года, в которых, в частности, подчеркивается необходимость большей транспарентности и подтверждается важность мер укрепления доверия как средства, способствующего обеспечению достижения цели предотвращения гонки вооружений в космическом пространстве,

напоминая о докладе Генерального секретаря от 15 октября 1993 года, который был представлен Генеральной Ассамблее на ее сорок восьмой сессии и в приложении к которому содержится исследование правительственных экспертов о применении мер по укреплению доверия в космическом пространстве A/48/305 и Corr.1,

отмечая конструктивный характер обсуждения этой тематики на Конференции по разоружению в 2010 году, в том числе мнения, выраженные государствами-членами,

отмечая также внесение Китаем и Российской Федерацией на рассмотрение Конференции по разоружению проекта договора о

предотвращении размещения оружия в космическом пространстве, применения силы или угрозы силой в отношении космических объектов См. CD/1839,

отмечая далее представление Европейским союзом проекта кодекса поведения в космической деятельности,

отмечая вклад государств-членов, которые в соответствии с пунктом 1 резолюции 61/75, пунктом 2 резолюции 62/43, пунктом 2 резолюции 63/68 и пунктом 2 резолюции 64/49 представили Генеральному секретарю конкретные предложения по международным мерам транспарентности и укрепления доверия в космосе,

1. *принимает к сведению* заключительный доклад Генерального секретаря, содержащий конкретные предложения государств-членов по международным мерам транспарентности и укрепления доверия в космосе A/65/123;

2. *просит* Генерального секретаря учредить на основе справедливого географического распределения группу правительственных экспертов для проведения, начиная с 2012 года, исследования о мерах транспарентности и укрепления доверия в космосе с использованием соответствующих докладов Генерального секретаря, включая доклад, представленный Генеральной Ассамблее на ее 65-й сессии, и без ущерба для субстантивной работы по проблематике предотвращения гонки вооружений в космическом пространстве в рамках Конференции по разоружению, и представить Генеральной Ассамблее на ее шестьдесят восьмой сессии доклад, содержащий в приложении к нему исследование группы правительственных экспертов;

3. *просит* Генерального секретаря предоставить группе правительственных экспертов любую помощь и услуги в рамках имеющихся ресурсов, которые могут понадобиться для осуществления ее задач;

4. *постановляет* включить в предварительную повестку дня своей шестьдесят шестой сессии пункт, озаглавленный "Меры по обеспечению транспарентности и укреплению доверия в космической деятельности".

ГЛОБАЛЬНАЯ БЕЗОПАСНОСТЬ:
ИННОВАЦИОННЫЕ МЕТОДЫ
АНАЛИЗА КОНФЛИКТОВ

Под общей редакцией А.И.СМИРНОВА

Корректура, дизайн обложки, верстка И.Кохтюлина

Подписано в печать 20.01.2011 г. Формат 60х90/16
Печ.л. 17,0. Тираж 2000. Заказ № _____

Общество «Знание» России
101990, Москва, Новая пл., д.3/4.
Тел. (495) 621-90-58, факс (495) 625-42-49
e-mail: znanie@znanie.org

Отпечатано в ОАО «Рыбинский Дом печати»
152901, г.Рыбинск, ул. Чкалова, 8.