ГЛОБАЛЬНАЯ БЕЗОПАСНОСТЬ
в ЦИФРОВУЮ ЭПОХУ:
СТРАТАГЕМЫ ДЛЯ РОССИИ

Под общей редакцией
Президента Национального института
исследований глобальной безопасности,
Председателя Отделения «Информационная глобализация»
Российской академии естественных наук,
доктора исторических наук, профессора

А.И.СМИРНОВА

Москва 2014

ББК 66.2
УДК 327
С 50

Рецензенты:

Аникин В.И. – доктор экономических наук, профессор
Кретов В.С. – доктор технических наук, профессор
Смульский С.В. – доктор политических наук, профессор

Авторский коллектив:
д.и.н. А.И. Смирнов (введение, гл.1, 5, 6, заключение)
к.т.н. В.Р. Григорьев (гл. 4)
к.полит.н. И.Н. Кохтюлина (гл. 3, 7, 8)
к.в.н. Б.В. Куроедов, О.В. Сандаров (гл. 2)

С 50 Глобальная безопасность в цифровую эпоху: стратагемы для России. Под общ. ред. Смирнова А.И. – М. : ВНИИгеосистем, 2014. – 394 с. : ил.

ISBN 978-5-8481-0172-0

Цифровая эпоха диктует свои правила обеспечения национальной безопасности в тесной увязке с международной. В книге системно рассматриваются мегатренды развития ИКТ как локомотива социализации человечества, а также сетевая мощь государств.

Предметно анализируются «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». Особое внимание уделено позиции России в вопросах угроз использования ИКТ на военно-политическом треке, а также для вмешательства во внутренние дела суверенных государств.

В книге исследуются такие актуальные проблемы, как кибершпионаж, кризисная и электронная дипломатия (с учетом зарубежного опыта).

С учетом стремительных процессов информационной глобализации работа может быть полезна для широкого круга читателей, интересующихся столь актуальными направлениями российской и мировой политики.

Global security in the digital age: stratagems for Russia
Edited by Anatoly Smirnov

The book is dedicated to the study of one of the most pressing challenges of the XXI century - the use of advanced information and communication technologies (ICT) in the modern global security matrix.

Digital era dictates the rules of national security - in close coordination with the international. The book systematically discusses megatrends ICT development as an engine of human socialization and the network power of states. Objectively analyzed «Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020». Particular attention is paid to the position of Russia in matters of ICT threats to military-political track, as well as interference in the internal affairs of sovereign states.

The book also examines topical issues such as cyber espionage, crisis and electronic diplomacy (including foreign experience).

Given the rapidity of information globalization the work can be useful for a wide range of readers interested in such current trends of Russian and world politics.

ISBN 978-5-8481-0172-0

К ЧИТАТЕЛЮ

Беспрецедентное развитие и распространение информационно-коммуникационных технологий (ИКТ) поражает своим охватом, количественными и качественными масштабами, но главное – тем влиянием, которое ИКТ оказывают на все сферы нашей жизни. Фактически информационное пространство стало «параллельным измерением» и даже «состоянием» жизни общества, которое отличается большей свободой, мобильностью, оперативностью, а подчас и меньшей ответственностью.

Однако технический прогресс порождает и угрозы индивидуальной, коллективной и национальной безопасности, которые по своим масштабам могут быть сопоставимы с угрозами применения обычного оружия или даже оружия массового уничтожения, а их последствия представляются не менее разорительными и разрушительными.

Мы все являемся свидетелями того деструктивного влияния, которое ИКТ могу оказывать на нашу жизнь. Это наглядно продемонстрировали такие события как электронные атаки на иранские ядерные объекты посредством вируса «Stuxnet», тенденциозная утечка информации через сайт «Викиликс», беспорядки и полномасштабные конфликты, спровоцированные через социальные сети, и, наконец, откровения Э.Сноудена.

Но одной из наиболее острых и опасных в стратегическом плане является проблема возможного применения ИКТ и, в частности, Интернета в целях, не совместимых с задачами обеспечения международной и национальной стабильности и безопасности. Становится очевидным, что «поигрывание технологическими мускулами» толкает человечество в сторону конфронтации.

В противовес такому милитаристскому подходу Россия продвигает на международной арене целый ряд миротворческих инициатив в сфере международной информационной безопасности (МИБ). Среди них проект «Правил поведения в области обеспечения МИБ» и Концепция конвенции об обеспечении международной информационной безопасности, призванные повысить уровень ответственности государств за их действия, установить «правила честной игры» в информационной сфере.

Россия поддерживает центральную роль ООН как ключевой площадки в обсуждении темы МИБ. В Первом комитете ГА ООН и Группе правительственных экспертов (ГПЭ) ООН по МИБ уже на регулярной основе идет диалог по наиболее острым и практически значимым вопросам повестки дня МИБ. В докладе ГПЭ, принятом в 2013 г., закреплен тезис о заинтересованности всех стран в развитии ИКТ в мирных целях, а также в предотвращении конфликтов, вызванных их применением.

В этом контексте особую роль приобретает мнение экспертного сообщества. Взвешенная, научно-обоснованная и – что самое главное – объ-

ективная и непредвзятая экспертиза в сфере МИБ востребована на самом высоком международном уровне. Как представляется, исследования, проведенные АНО «Национальный институт исследований глобальной безопасности» (НИИГлоБ), весьма актуальны и информативны. Несомненный интерес представляет глава о мегатрендах цифровой эпохи. Детально проработаны вопросы, связанные с геополитическими вызовами цифровой эры с учетом потенциала в сфере ИКТ ведущих стран мира.

Под МИБ в данной работе понимается такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

Следуя структуре угроз в области МИБ в соответствии с «Основами государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» (утверждены Президентом РФ 24 июля 2013 г. Пр-1753) в книге рассмотрено использование ИКТ:

а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

б) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

г) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

В работе исследована все возрастающая роль так называемой «мягкой силы», в т.ч. в контексте подготовки и реализации «цветных» революций. Безусловный интерес у читателя вызовет анализ виртуального «украинского фронта». С учетом разоблачений Э.Сноудена подробно проанализированы программы глобальной слежки спецслужб США и их союзников.

Принимая во внимание рост конфликтного потенциала в мире, интерес представляет анализ системы ситуационно-кризисного реагирования, в т.ч. на примерах ряда европейских стран.

Безусловно, полезными для читателей будут представленные в заключении конкретные предложения по использованию новейших ИКТ и укреплению информационной безопасности в России.

Специальный представитель
Президента Российской Федерации
по вопросам международного
сотрудничества в области
информационной безопасности,
посол по особым поручениям,
доктор исторических наук, профессор А. КРУТСКИХ

СОДЕРЖАНИЕ

«Накал военно-политической, экономической, информационной конкуренции в мире не снижается, а только усиливается. И другие центры влияния внимательно следят за усилением России».

Послание Президента Российской Федерации Федеральному Собранию, 12 декабря 2013 года

ВВЕДЕНИЕ

Начало XXI века 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, социогенные, природогенные и техногенные катастрофы, эпидемии и пандемии – вот далеко не полный перечень его трагедий.

Все более возрастающее значение в матрице глобальной безопасности приобретают инфогенные риски и угрозы.

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» [1].

Вот уже более полувека весь мир охвачен беспрецедентной информационной революцией. Пронизывая практически все страты человечества, она, наряду с несомненным позитивом, резко обострила геополитическую турбулентность.

Попытки осмысления и прогнозирования глобальных катаклизм предпринимает интеллектуальная элита всего мира. Особое место в анализе занимает проблематика роли новейших информационно-коммуникационных технологий (ИКТ) в геополитических явлениях.

[1] http://www.scrf.gov.ru/documents/1/99.html дата обращения 20 июля 2013 г.

С учетом того, что монография «Информационная глобализация и Россия: вызовы и возможности»[2] (неожиданно удостоенная медали и диплома 9-й всероссийской конференции по информационной безопасности «ИНФОФОРУМ» в номинации «публикация года» 2007 г.) вызвала значительный интерес, в 2011 г. мною совместно с коллегами была написана книга-продолжение «Глобальная безопасность: инновационные методы анализа конфликтов»[3].

Её суть в том, что, в условиях стремительных перемен в мире 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 оговориться, что в качестве сотрудника Международного отдела ЦК КПСС мне довелось участвовать в ряде ситанализов во второй половине 1980-х гг. по методу, разработанному Е.М.Примаковым, В.И.Гантманом и В.И.Любченко.

Указанный метод продолжает использоваться в ситуационно-кризисных центрах (СКЦ), оснащенных новейшими ИКТ, в т.ч. информационно-аналитическими системами, позволяющими в онлайне вести контент-, ивент- и коннект-анализ мультимедийной информации, а также социальных сетей и мемов на десятках иностранных языках о «горячих точках» в мире. Это позволяет прогнозировать их развитие, а также, опираясь на базы знаний, вносить лицу, принимающему решение (ЛПР), оптимальные предложения по реагированию на них (в т.ч. с визуализацией).

Обсуждение данной проблематики, в т.ч. на международных конференциях под эгидой ОДКБ, ШОС, Баренцинститута (Норвегия), РСМД, «Инфофорума», МГИМО(У), МГУ им. М.В.Ломоносова, Общества «Знание» России, Правительства Санкт-Петербурга, на мастер-классах в НИЯУ МИФИ, Северном (Арктическом) федеральном университете

[2] См. http://niiglob.ru/index.php/ru/2011-01-15-10-08-52/180-2011-02-26-19-32-38.html
[3] См. http://niiglob.ru/index.php/ru/2011-01-15-10-08-52/181-2011-02-26-20-14-44.html

им. М.В.Ломоносова, РАНХиГС при Президенте России и других площадках показали, что многие коллеги не совсем ясно представляли себе глобальные угрозы и возможности, вытекающие из применения арсенала «мягкой силы» интерактивного поколения, т.е. «мягкой силы 2.0».

Интерес к теме резко обострился в связи с так называемой «Арабской весной», а также «цветными революциями» на постсоветском пространстве. Начинались они не без влияния цифровых технологий, а заканчивались - вспышками вооруженного противостояния, массового насилия, кровопролития и государственными переворотами.

С учетом вышеизложенного, Национальным институтом исследований глобальной безопасности (НИИГлоБ) была подготовлена книга «Глобальная безопасность и «мягкая сила 2.0»: вызовы и возможности для России»[4], которая вышла в свет в сентябре 2012 г.

Презентация книги, а также изложение её материалов на многочисленных международных и отечественных площадках, показала её достаточно высокую востребованность, как в экспертном сообществе, так и среди читателей.

Вместе с тем, выход пятого издания прогноза Национального совета по разведке США «Глобальные тенденции 2030: Альтернативные миры»[5], утверждение 12 февраля 2013 г. новой редакции Концепции внешней политики России[6], разработка НАТО документа «Таллинское руководство по ведению кибервойн», а также анализ беспрецедентных разоблачений Э.Сноудена о глобальном кибершпионаже США, побудил продолжить исследование столь острой геополитической проблемы.

---

[4] См. http://niiglob.ru/index.php/ru/2011-01-15-10-08-52/307-globalnaya-bezopasnost-i-qmyagkaya-sila-20q-vyzovy-i-vozmozhnosti-dlya-rossii.html

[5] http://www.dni.gov/index.php/about/organization/global-trends-2030 дата посещения 21.07.2013

[6] http://www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/c32577ca0017434944257b160051bf7f!OpenDocument дата посещения 21.07.2013

Особую роль в выработке структуры работы сыграли «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года», утвержденные В.В.Путиным 24 июля 2013 г.[7]

В силу этого в данной работе поставлена цель максимально кратко обобщить предыдущие исследования, а основное внимание сконцентрировать на мегатрендах глобальных угроз в цифровую эпоху, а также позиции России по укреплению международной и национальной безопасности.

Следует отметить, что в последнее время рядом отечественных и зарубежных экспертов уже были предприняты попытки рассмотреть данную проблему.

Очень полезными стали материалы конвентов РАМИ под общей редакцией ректора МГИМО(У), акад. РАН А.В.Торкунова, его труд «По дороге в будущее», а также работа А.И.Подберезкина «Евразийская воздушно-космическая оборона»[8].

В книге использованы исследование Института информационной безопасности МГУ им. М.В.Ломоносова[9], работа Ричарда Кларка[10], В.И.Анненкова[11], В.В.Карякина[12] и др. Особо полезен был инновационный труд Т.А.Шаклеиной и А.А.Байкова[13].

---

[7] http://www.scrf.gov.ru/documents/6/114.html дата посещения 31.12.2013

[8] Подберезкин А.И. Евразийская воздушно-космическая оборона. М.: МГИМО-Университет, 2013. - 488 с. http://eurasian-defence.ru/node/23123 22.06.2014

[9] Казарин О.В., Сальников А.А., Шаряпов Р.А., Ященко В.В. «Новые акторы и безопасность в киберпространстве. Вестник Московского университета. Серия 12. Политические науки. 2010. Часть 1: № 2, с.71-84. Часть 2: № 3, с.90-103

[10] Третья мировая война. Какой она будет? Cyber War: The Next Threat to National Security and What to Do About It Питер.-2011.336 с.

[11] Сетецентризм: геополитические и военно-политические аспекты современности/ Под общ. Ред. Проф. Анненкова В.И. Учебник. -М. РУСАВИА. 2013. - 496 с.

[12] Карякин В.В. Геополитика третьей волны: трансформация мира в эпоху Постмодерна. - М.:2013. - 432 с.

[13] Мегатренды: Основные траектории эволюции мирового порядка в XXI веке: Учебник / Под. ред. Т.А.Шаклеиной, А.А.Байкова. - М.:ЗАО Издательство «Аспект Пресс». 2013. - 448 с.

Чрезвычайно интересен проект «Политический атлас современности», предпринятый МГИМО(У) МИД России в котором, наряду с методами политической компаративистики, используются различные методы многомерного статистического анализа (регрессионный, дискриминантный, кластерный, метод главных компонент и др.).

Развитие данного проекта способно стать одним из системообразующих центров всей отечественной школы международных исследований.

Полезными для исследования стали коллективные работы ИМЭМО, Института проблем управления, Института Европы, Института системного анализа, Кольского научного центра РАН, ПИР-центра, а также Рабочая тетрадь РСМД «Россия и вызовы цифровой среды»[14].

Особого внимания заслуживает труд Института экономических стратегий «Глобальный рейтинг интегральной мощи 100 стран. Доклад - 2012 к обсуждению. 3-е издание»[15], т.к. методика стратегической матрицы показала высокую адаптивность к динамике международных отношений и мировой экономики.

Существенную помощь в анализе зарубежной и отечественной библиографии по классификации информационного оружия оказала работа В.К.Новикова[16], в том числе при исследовании «виртуального украинского фронта» - кризиса на Украине 2013-2014 гг.

Вышеназванные труды, а также многочисленные рейтинги, в т.ч. по интегральной силе государств, по «мягкой силе», «электронной дипломатии» и др. реферативно применены в данной монографии. Естественно, что при этом приняты во внимание основополагающие документы внешней и внутрен-

[14] http://russiancouncil.ru/common/upload/WP15Cybersecurity-Ru.pdf 21.06.2014

[15] М.: Международная Академия исследований будущего, Институт экономических стратегий, 2012. - 108 с.

[16] Новиков В.К. Информационное оружие - оружие современных и будущих войн.- 2-е изд. испр. - М.: Горячая линия-Телеком, 2013.- 262 с.: ил.

ней политики России: Стратегия национальной безопасности до 2020 года, новая редакция Концепция внешней политики, Военная доктрина, Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» и др.

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

Особое место занимают указы и выступления Президента Российской Федерации по международной проблематике. Так, на совещании с российскими послами и постоянными представителями при международных организациях 9 июля 2012 г. президент России подчеркнул, что «…по части использования новых технологий, например, так называемой «мягкой силы», безусловно, есть над чем подумать» [17].

О конкретных путях повышения эффективности «мягкой силы» России шла речь на совещании в Москве (3-4 сентября 2012 г.) руководителей российских центров науки и культуры и представителей Россотрудничества, что позднее нашло отражение в Указе Президента России от 8 мая 2013 г. № 476.

Завершая введение, хотелось бы подчеркнуть, что данная работа является лишь попыткой анализа мегатрендов глобальной безопасности в цифровую эпоху, а также вызовов и возможностей для внешней политики России на треке резко обострившейся геополитической конкуренции и турбулентности.

[17] http://www.kremlin.ru/transcripts/15902

Авторский коллектив выражает искреннюю признательность рецензентам: заведующему кафедрой Национальной безопасности и государственного управления Дипломатической академии МИД России д.э.н., профессору Аникину В.И., профессору этой кафедры д.т.н. Кретову В.С., а также декану факультета Национальной безопасности РАНХиГС при Президенте России, д.полит.н., профессору Смульскому С.В. за полезные замечания и соображения, которые были с благодарностью учтены в работе.

Авторы надеются, что книга будет способствовать лучшему пониманию читателей позиции России в современных международных отношениях, а также будет востребована для продолжения исследований столь актуальной научной проблемы.

«Смена исторических эпох определяется
сменой коммуникационных технологий»

Герберт Маршалл Маклюэн
(канадский социолог)

1. МЕГАТРЕНДЫ ЦИФРОВОЙ ЭПОХИ

1.1. Вехи цивилизации: от пещеры до «Homo Informaticus»

Цивилизация стремительно вступила в цифровую эру своего развития. Постулируемый тезис подтверждается нижеследующим синопсисом эволюции человечества, которое обитает на планете порядка 50 тысяч лет, т.е. сменилось около 1600 поколений. Из них:

- 1100 - провели жизнь в пещерах;
- 800 - применяют огонь;
- 400 - используют энергию животных;
- 300 - владеют энергией воды и ветра;
- 150 - осуществляют эффективную связь поколений благодаря письменности (из них 12 - через печатное слово);
- 16 - применяют порох;
- 8 - измеряют точное время;
- 6 - используют искусственные источники энергии;
- 4 - применяют электромоторы;
- 2 - владеют атомной энергией, реактивной авиацией, телевидением, лазерами, антибиотиками.

И только одно поколение применяет персональные компьютеры, Интернет, космические, генные, когнитивные и нанотехнологии.

Данное поколение некоторые эксперты называют **поколением информационной глобализации[18], его представителей - «Homo Informaticus», а молодежь - «цифровыми аборигенами».**

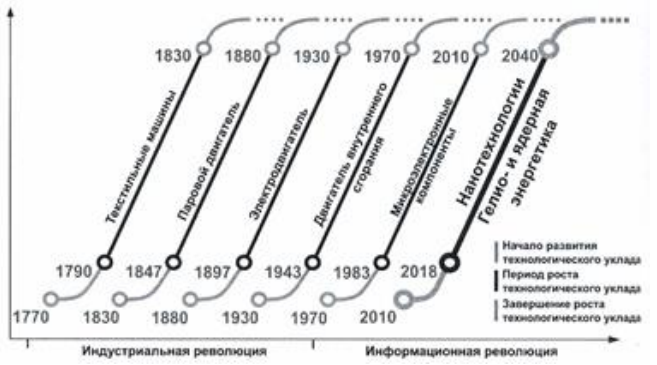
1.2. ИКТ – локомотив пятого технологического уклада человечества

1.2.1. Понятие «технологический уклад» и основные этапы эволюции укладов

Используя термин «технологический уклад» (комплекс технологий, изобретений и инноваций, лежащих в основе количественного и качественного скачка в развитии производительных сил общества), можно констатировать, что **человечество, пройдя пять технологических укладов, входит в шестой.**

Наиболее четко схему технологических укладов с указанием характерных технологий представил академик РАН С.Ю.Глазьев[19] (схема 1.1.).

Схема 1.1.



[18] Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности. - М. Изд. Дом «Парад». 2005. С.8-9

[19] Глазьев С.Ю. Уроки современной революции: крах либеральной утопии и шанс на «экономическое чудо»/С.Ю. Глазьев.-М. Издательский дом «Экономическая газета», 2011.- С.330

Рассмотрим кратко их сущность.

Первый технологический уклад (революция) происходил в разных странах в 1785–1843 гг., но раньше всего - в Англии. Уклад характеризовался изобретением прядильных и ткацких станков, использованием энергии воды и ветра в мельницах, а также созданием приводов для различных механизмов.

Второй технологический уклад был основан на изобретении Д.Уаттом универсальной паровой машины, которая могла быть использована как двигатель для любого механизма. В XIX веке паровой двигатель применялся в качестве платформы для паровозов, пароходов, прядильных и ткацких станков, паровых мельниц, парового молота и т.д. Изобретение паровой машины доказывает справедливость китайской формулы «инвестиционного счастья», ибо русский механик Ползунов изобрел паровую машину раньше Уатта, но в России она оказалась не нужна и о ней забыли, как и о других «несвоевременных» изобретениях.

Третий технологический уклад охватывает период конца XIX середины XX века. Предметом глобальной конкуренции стали электрические машины и механизмы, встроенные в новые средства производства, а также двигательная сила электричества (её научились получать еще в 30-х годах XIX века). Ключевым моментом наступления нового технологического уклада стало изобретение Т.Эдисоном лампочки и его последующих действий как гениального предпринимателя и технолога по созданию частных компаний, применяющих электрический ресурс.

Человечество получило в свое распоряжение телеграф, радиосвязь, бытовую технику и т.д.

Четвертый технологический уклад (XX век) возник в недрах «электрического» уклада и стал использовать знания и технологии, направленные на превращение энергии углеводородов в универсальную двигательную силу. Появились двигатели внутреннего сгорания и на этой платформе были

построены автомобили, тракторы, самолеты, корабли, подводные лодки и другие машины и механизмы. Начала свое развитие ядерная энергетика задолго до ее использования в экономике стран.

Следует отметить, что единственный раз в отечественной истории СССР удалось в кратчайшие сроки освоить предметы конкуренции четвертого технологического уклада, в частности, в области вооружений. Это произошло благодаря огромным ресурсам страны, а также грамотным действиям власти, направленным на создание технологических цепочек предприятий, разделение труда, своевременную подготовку компетентных кадров, использование лучших стандартов и учет опыта США и Германии в производстве вооружений.

1.2.2. Основные тренды пятого технологического уклада

Принято считать, что пятый технологический уклад стартовал не в 1946 г. с созданием первого компьютера, а в 1956 г., когда американскими физиками был изобретен транзистор. Транзистор совершил революцию в технологии радио, привел к созданию микросхем, микропроцессоров, компьютеров и многих других телекоммуникационных систем. Это был выход из «первобытного механического» века в век электронный, космический и компьютерный.

На этом этапе впервые в истории предмет конкуренции (знания, технологии и производство) перестал служить целям простой замены человеческого труда двигательной силой машин, как в предыдущих укладах. Вместо этого **предмет конкуренции стал служить целям развития доселе неизвестных интеллектуальных сил массовой автоматизации производства, проектирования изделий и управления предприятием.** Стал закладываться принципиально другой способ преобразования ресурсов в интеллектуальную силу. В

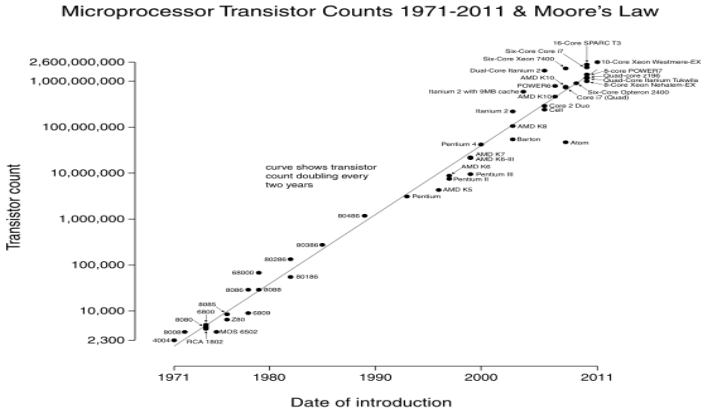
жизнь человека вошли Интернет, мобильный телефон и иные гаджеты и сервисы.

1.2.2.1. Закон Мура

Лауреат Нобелевской премии по физике 2000 г. Ж.И.Алферов считает ИКТ самой динамичной отраслью экономики в мире, т.к. темпы её роста в три раза выше темпов ростов ВВП.[20]

Наиболее ярко динамика ИКТ прослеживается на примере так называемого закона Мура. Инженер Гордон Мур эмпирически описал удвоение числа транзисторов на кристалле микропроцессора каждые два года.[21] Вертикальная ось имеет логарифмическую (!) шкалу, то есть кривая соответствует экспоненциальному закону - количество транзисторов удваивается практически каждые 2 года (схема 1.2.).[22]

Схема 1.2.



[20] Алферов Ж.И. Отрасль отчаяния, отрасль надежды //Экономическая философская газета. 08.06.2004. № 22

[21] Часто цитируемый интервал в 18 месяцев связан с прогнозом Давида Хауса из Intel, по мнению которого производительность процессоров должна удваиваться каждые 18 месяцев из-за сочетания роста количества транзисторов и быстродействия каждого из них.

[22] http://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BA%D0%BE%D0%BD_%D0%9C%D1%83%D1%80%D0%B0 10.01.2014

1.2.2.2. Измерение информационного общества Международным союзом электросвязи

Международный союз электросвязи (International Telecommunication Union, ITU), специализированное подразделение ООН в области ИКТ, исследовал развитие ИКТ в странах мира в период с 2011 по 2012 год.[23] Результатом стал доклад «Измерение информационного общества 2013» (Measuring the Information Society 2013), содержащий рейтинг развития 157 стран в сфере ИКТ. Впереди - третий год подряд Южная Корея, **у России - 40 место**.

Индекс развития ИКТ (ICT Development Index) разработан в 2007 г. на основе 11 показателей и сводится в единый критерий, который можно использовать для проведения сравнительного анализа на глобальном, региональном и национальном уровнях. Эти показатели касаются доступа к ИКТ, их использования, а также практического знания этих технологий, в т.ч.: число стационарных и мобильных телефонов на 100 жителей страны, количество домашних хозяйств, имеющих компьютер, количество пользователей Интернета, уровни грамотности и т.д.

Первые 30 мест в рейтинге занимают страны с высоким уровнем дохода, что говорит о прочной взаимосвязи между доходом и прогрессом в области ИКТ. Практически две трети из 30 ведущих в рейтинге стран - европейские, где совместная нормативно-правовая база и четкий набор приоритетных областей деятельности, целей и задач помогли им превратиться в передовые информационные экономики. К числу 30 ведущих стран относятся также экономики с высоким уровнем доходов из Азиатско-Тихоокеанского региона (Австралия, Макао (Китай), Сингапур и Новая Зеландия), а также США, Канада и Барбадос из региона Северной и Южной Америки.

[23] http://www.itu.int/ 10.01.2014

Несмотря на широкое распространение ИКТ во всем мире, налицо значительные различия между развитыми и развивающимися странами, причем значения Индекса в среднем вдвое выше в развитом мире, чем в развивающихся странах. В отчете определена группа регионов с наиболее низкими уровнями развития ИКТ, в которых проживают 2,4 миллиарда человек, и подчеркивается, что государственным институтам необходимо уделять пристальное внимание этой группе. К числу таких регионов относятся африканские страны, а также некоторые густонаселенные районы Индии, Пакистана и др.

В докладе также отмечены страны, которые стремительно сокращают «цифровой разрыв». К их числу относятся: ОАЭ, Барбадос, Сейшельские Острова, Беларусь, Коста-Рика, Монголия, Замбия, Австралия, Бангладеш, Оман и Зимбабве.

1.2.2.2.1. Индекс развития ИКТ в странах мира 2013 г.[24]

Таблица 1.1.

РЕЙТИНГ	СТРАНА	ИНДЕКС
1	Южная Корея	8,57
2	Швеция	8,45
3	Исландия	8,36
4	Дания	8,35
5	Финляндия	8,24
6	Норвегия	8,13
7	Нидерланды	8,00
8	Великобритания	7,98
9	Люксембург	7,93
10	Гонконг	7,92
11	Австралия	7,90
12	Япония	7,82
13	Швейцария	7,78

[24] http://www.itu.int/ 10.01.2014

РЕЙТИНГ	СТРАНА	ИНДЕКС
14	Макао	7,65
15	Сингапур	7,65
16	Новая Зеландия	7,64
17	Соединенные Штаты Америки	7,53
18	Франция	7,53
19	Германия	7,46
20	Канада	7,38
21	Австрия	7,36
22	Эстония	7,28
23	Ирландия	7,25
24	Мальта	7,25
25	Бельгия	7,16
26	Израиль	7,11
27	Испания	6,89
28	Словения	6,76
29	Барбадос	6,65
30	Италия	6,57
31	Катар	6,54
32	Греция	6,45
33	Объединенные Арабские Эмираты	6,41
34	Чехия	6,40
35	Латвия	6,36
36	Португалия	6,32
37	Польша	6,31
38	Хорватия	6,31
39	Бахрейн	6,30
40	Россия	6,19
41	Беларусь	6,11
42	Венгрия	6,10
43	Словакия	6,05
44	Литва	5,88
45	Кипр	5,86
46	Болгария	5,83
47	Уругвай	5,76

РЕЙТИНГ	СТРАНА	ИНДЕКС
48	Казахстан	5,74
49	Антигуа и Барбуда	5,74
50	Саудовская Аравия	5,69
51	Чили	5,46
52	Ливан	5,37
53	Аргентина	5,36
54	Оман	5,36
55	Румыния	5,35
56	Сербия	5,34
57	Македония	5,19
58	Бруней	5,06
59	Малайзия	5,04
60	Коста-Рика	5,03
61	Азербайджан	5,01
62	Бразилия	5,00
63	Сент-Винсент	4,81
64	Сейшельские Острова	4,75
65	Молдова	4,74
66	Тринидад и Тобаго	4,73
67	Босния и Герцеговина	4,71
68	Украина	4,64
69	Турция	4,64
70	Панама	4,61
71	Грузия	4,59
72	Маврикий	4,55
73	Мальдивы	4,53
74	Армения	4,45
75	Сент-Люсия	4,43
76	Иордания	4,22
77	Колумбия	4,20
78	Китай	4,18
79	Венесуэла	4,17
80	Албания	4,11
81	Эквадор	4,08

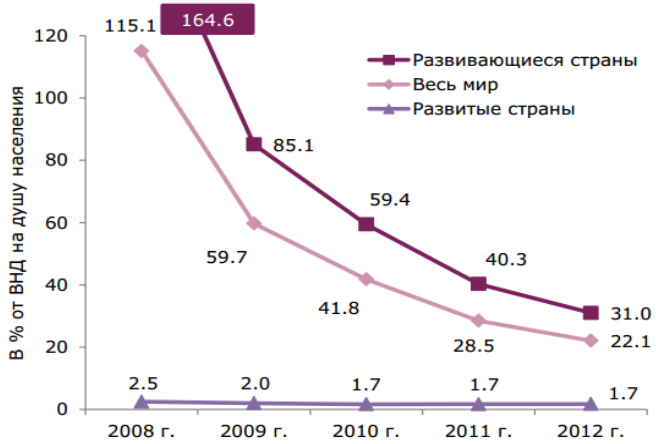
РЕЙТИНГ	СТРАНА	ИНДЕКС
82	Фиджи	3,99
83	Мексика	3,95
84	Южная Африка	3,95
85	Монголия	3,92
86	Египет	3,85
87	Суринам	3,84
88	Вьетнам	3,80
89	Марокко	3,79
90	Иран	3,79
91	Тунис	3,70
92	Перу	3,68
93	Ямайка	3,68
94	Доминикана	3,58
95	Таиланд	3,54
96	Кабо-Верде	3,53
97	Индонезия	3,43
98	Филиппины	3,34
99	Боливия	3,28
100	Сальвадор	3,25
101	Тонга	3,23
102	Сирия	3,22
103	Парагвай	3,21
104	Узбекистан	3,12
105	Гайана	3,08
106	Алжир	3,07
107	Шри-Ланка	3,06
108	Ботсвана	3,00
109	Намибия	2,85
110	Гондурас	2,74
111	Куба	2,72
112	Габон	2,61
113	Гана	2,60
114	Никарагуа	2,54
115	Зимбабве	2,52

РЕЙТИНГ	СТРАНА	ИНДЕКС
116	Кения	2,46
117	Свазиленд	2,44
118	Бутан	2,40
119	Судан	2,33
120	Камбоджа	2,30
121	Индия	2,21
122	Нигерия	2,18
123	Лаос	2,10
124	Сенегал	2,02
125	Соломоновы Острова	1,97
126	Лесото	1,95
127	Йемен	1,89
128	Гамбия	1,88
129	Пакистан	1,83
130	Уганда	1,81
131	Джибути	1,77
132	Замбия	1,77
133	Мавритания	1,76
134	Мьянма	1,74
135	Бангладеш	1,73
136	Камерун	1,72
137	Кот-д'Ивуар	1,70
138	Коморские Острова	1,70
139	Ангола	1,68
140	Конго	1,66
141	Руанда	1,66
142	Танзания	1,65
143	Бенин	1,60
144	Мали	1,54
145	Малави	1,43
146	Либерия	1,39
147	Демократическая Республика Конго	1,31
148	Мозамбик	1,31
149	Мадагаскар	1,28

РЕЙТИНГ	СТРАНА	ИНДЕКС
150	Гвинея-Бисау	1,26
151	Эфиопия	1,24
152	Гвинея	1,23
153	Эритрея	1,20
154	Буркина Фасо	1,18
155	Чад	1,01
156	Центрально-Африканская Республика	1,00
157	Нигер	0,99

Из диаграммы ниже видно, что распространение ИКТ стимулируется постоянным снижением расценок на услуги телефонии и широкополосного Интернета.

Диаграмма 1.1.



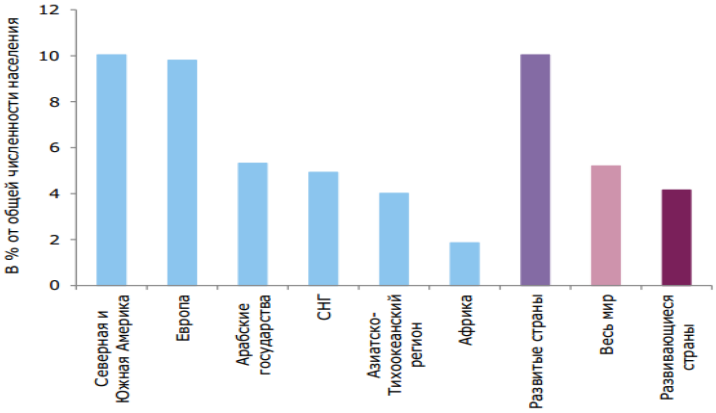
Источник: МСЭ. Значения ВНД на душу населения основаны на данных Всемирного банка. Примечание. – Среднеарифметические значения. Основано на данных по 144 экономикам, по которым имелись данные о ценах на фиксированную широкополосную связь за 2008, 2009, 2010, 2011 и 2012 годы.

МСЭ особое внимание уделяет анализу роли «цифровых аборигенов». Как видно из графика СНГ на этом треке значи-

тельно уступает развитым экономикам и, даже, арабским странам (диаграмма 1.2.).

Диаграмма 1.2.

«Цифровые аборигены» в процентах от общей численности населения, в разбивке по регионам и уровням развития, конец 2012 года



Источник: МСЭ.

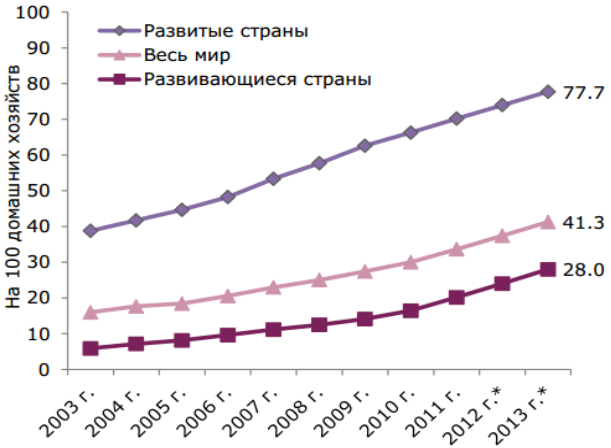
1.2.2.2.2. Тренды охвата планеты Интернетом и мобильной связью

Как видно из диаграммы 1.3., в конце 2013 г. к Интернету подключены 2,7 миллиарда человек (почти 40% населения мира). При этом доля подключенного населения в развитых странах достигла почти 77% по сравнению с 31% в развивающихся странах, а цены на фиксированную широкополосную связь в процентах от ВНД на душу населения, упали за четыре года на 82%.[25]

[25] http://www.itu.int/net/pressoffice/press_releases/2013/pdf/41-ru.pdf

Диаграмма 1.3.

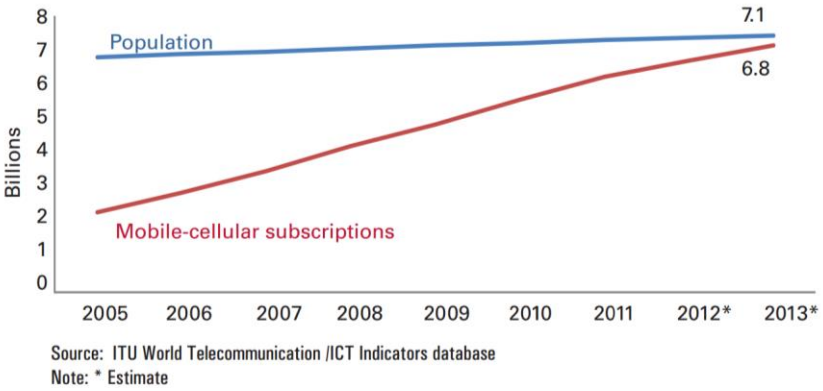
Процент домашних хозяйств, имеющих доступ в Интернет, в разбивке по уровням развития, 2003-2013 гг.



Источник: МСЭ.
Примечание. – *Оценка.

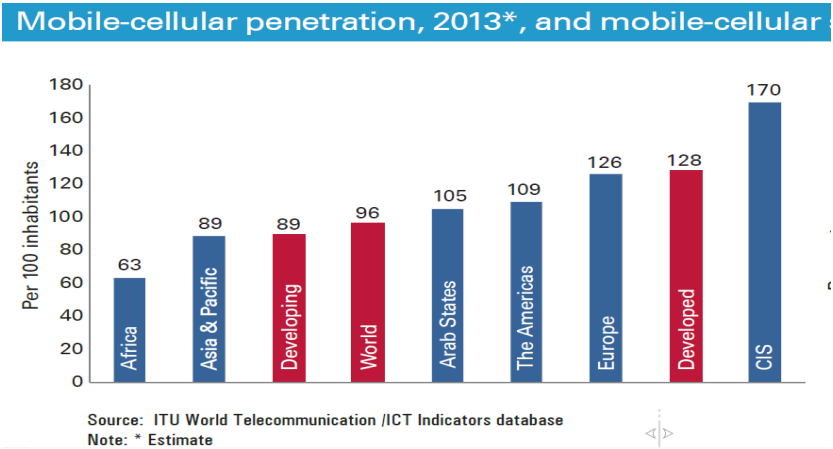
Анализ нижеследующих диаграмм показывает, что человечество вплотную подошло к полному охвату мобильной связью. Однако это количественный подход. В действительности, в ряде стран охват значительно ниже. «Выручают» страны, где на каждого жителя приходится более одной сим-карты.

Диаграмма 1.4.



Source: ITU World Telecommunication /ICT Indicators database
Note: * Estimate

Диаграмма 1.5.



Source: ITU World Telecommunication /ICT Indicators database
Note: * Estimate

1.2.2.3. Анализ карты проникновения «глобальной паутины» Оксфордского института Интернета

Оксфордский институт интернета (Oxford Internet Institute) представил очередную карту мира (первую - в 2008 г.), со-

ставленную по количеству проживающих в странах пользователей «мировой паутиной» (рис. 1.1.)[26]. По некоторым параметрам, Россия занимает на ней достаточно скромное место[27].

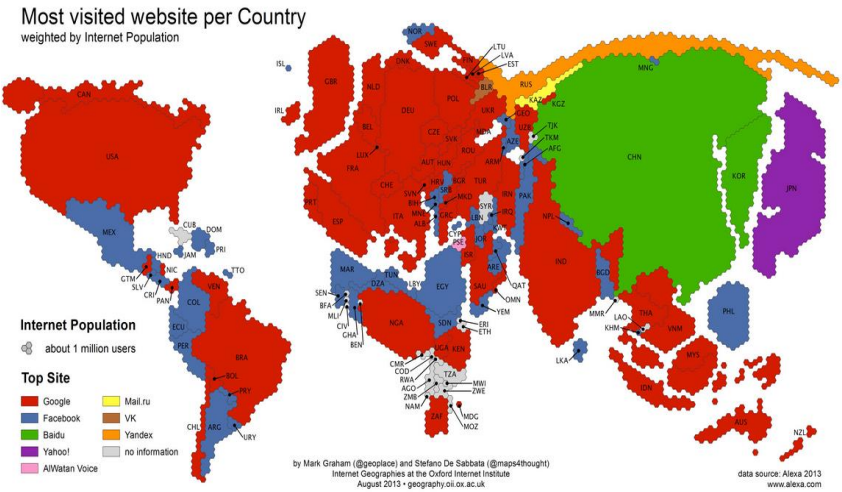


Рис. 1.1.

Для обозначения данных здесь используют всего два показателя. **Размер страны определяется количеством Интернет-пользователей, а интенсивность цвета отображает процентное соотношение любителей интернета в стране ко всему населению.**

По первому параметру от России и Канады остались на данной карте только тонкие полоски. В то время как Китай, судя по выделенной ему территории, стал лидером среди мировых Интернет-держав.

По второму критерию у России 40-60% Интернет-активного населения, а у Китая он на уровне 20-40%. Странами, где процент населения, охваченного Интернетом, превы-

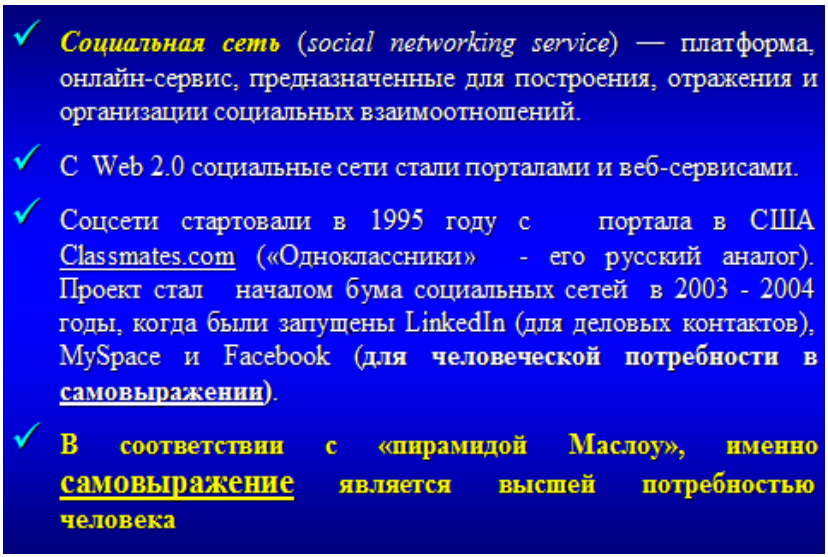
[26] http://www.rg.ru/2013/10/12/oxford-site-anons.html дата обращения 11.01.2014
[27] http://geography.oii.ox.ac.uk/#internet-population-and-penetration, дата обращения 11.01.2014

сил 80, стали Великобритания, Канада, Новая Зеландия, Исландия, Катар, Южная Корея, Германия, Нидерланды, Дания, Чехия и страны Скандинавии.

В Азии проживают 42 процента всех пользователей Интернета в мире и, с учетом густонаселенности, здесь имеется существенный потенциал роста.

1.2.2.3. Распространение социальных сетей в мире

1.2.2.3.1. Базовые понятия и термины



Потребности человека

- В 1943-м году философ Абрахам Маслоу опубликовал модель потребностей человека
  - Основные физиологические потребности (еда, сон, тепло, секс)
  - Безопасность (жилье, постоянная работа, здоровье, защищенность от опасностей)
  - Отношения (друзья, партнеры, любовь)
  - Признание (статус, власть, деньги)
  - Самореализация

1.2.2.3.2. Крупнейшие социальные сети по странам, охвату аудитории и количеству аккаунтов

Существует немало методик и ресурсов по анализу крупнейших глобальных социальных сетей, их аудитории, аккаунтов и т.д. Воспользуемся одним из них. Он дает следующую картину (рис. 1.2.).[28]

[28] http://www.alexa.com/

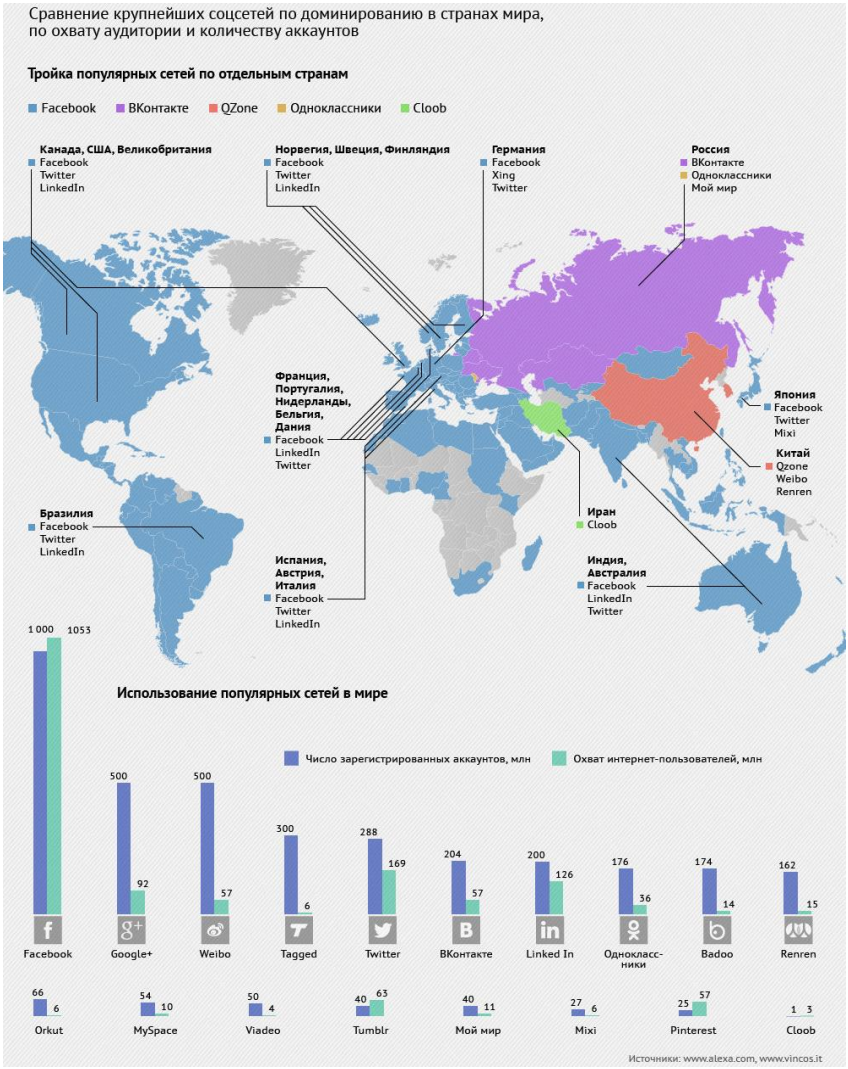
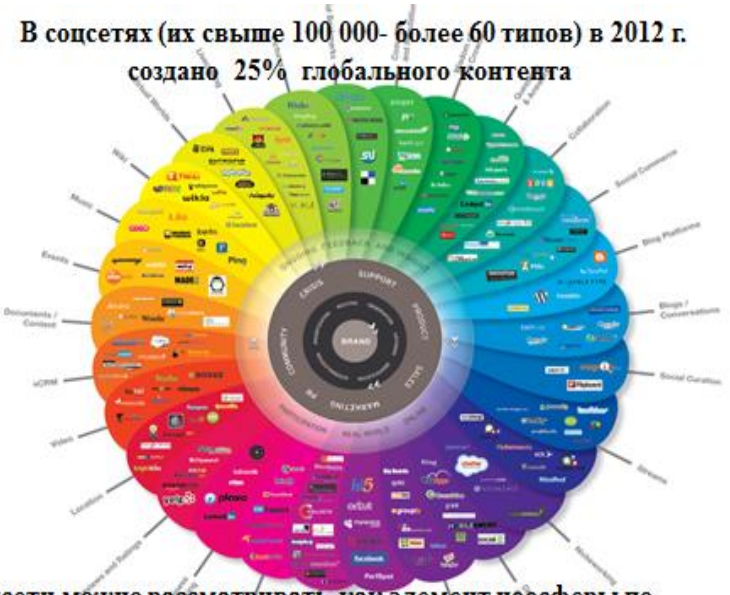

Сравнение крупнейших соцсетей по доминированию в странах мира,
по охвату аудитории и количеству аккаунтов
Тройка популярных сетей по отдельным странам
Facebook
ВКонтакте
QZone
Одноклассники
Cloob
Канада, США, Великобритания
Facebook
Twitter
LinkedIn
Норвегия, Швеция, Финляндия
Facebook
Twitter
LinkedIn
Германия
Facebook
Xing
Twitter
Россия
ВКонтакте
Одноклассники
Мой мир
Франция, Португалия, Нидерланды, Бельгия, Дания
Facebook
LinkedIn
Twitter
Япония
Facebook
Twitter
Mixi
Китай
Qzone
Weibo
Renren
Иран
Cloob
Бразилия
Facebook
Twitter
LinkedIn
Испания, Австрия, Италия
Facebook
Twitter
LinkedIn
Индия, Австралия
Facebook
LinkedIn
Twitter
Использование популярных сетей в мире
Число зарегистрированных аккаунтов, млн
Охват интернет-пользователей, млн
1 000
1053
500
92
500
57
300
6
288
169
204
57
200
126
176
36
174
14
162
15
Facebook
Google+
Weibo
Tagged
Twitter
ВКонтакте
Linked In
Однокласс-ники
Badoo
Renren
66
6
54
10
50
4
40
63
40
11
27
6
25
57
1
3
Orkut
MySpace
Viadeo
Tumblr
Мой мир
Mixi
Pinterest
Cloob
Источники: www.alexa.com, www.vincos.it

Рис. 1.2.

1.2.2.3.3. Социальные сети как элемент ноосферы по В.И.Вернадскому



1.3. Контуры шестого технологического уклада

1.3.1. Технологические уклады и длинные волны Н.Д. Кондратьева

Прежде чем перейти к шестому укладу, рассмотрим теорию советского экономиста Николая Дмитриевича Кондратьева (1892-1938). В 1920-е гг. он обратил внимание на то, что в долгосрочной динамике некоторых экономических индикаторов наблюдается определенная циклическая регулярность, в ходе которой на смену фазам роста соответствующих показателей приходят фазы их относительного спада с характерным

периодом этих долгосрочных колебаний порядка 50 лет. Такие колебания были обозначены им как большие или длинные циклы.

Впоследствии известный австрийско-американский экономист Й.Шумпетер в честь российского ученого назвал их кондратьевскими циклами. Их стали также называть длинными волнами, или кондратьевскими волнами, иногда К-волнами[29]. **Многие исследователи связывают смену циклов с технологическими укладами и называют циклы Кондратьева таблицей Менделеева для экономики.**[30]

Для периода после промышленной революции обычно выделяются следующие кондратьевские циклы/волны:

- 1 цикл - с 1803 до 1841-43 гг. (отмечены моменты минимумов экономических показателей мировой экономики);
- 2 цикл - с 1844-51 до 1890-96 гг.;
- 3 цикл - с 1891-96 до 1945-47 гг.;
- 4 цикл - с 1945-47 до 1981-83 гг.;
- 5 цикл - с 1981-83 до ~2018 г. (прогноз);
- 6 цикл - с ~2018 до ~ 2060 (прогноз).

1.3.1.1. Инфратраектории 4 и 5 волны Н.Д.Кондратьева как основы для шестой

Прорывные технологии открывают возможности для расширения производства и формируют новые секторы экономики, образующие новый технологический уклад. Иностранный член РАН, профессор Аскар Акаев даёт следующие инфратраектории четвертого и пятого циклов Кондратьева.[31]

[29] http://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D0%BA%D0%BB%D1%8B_%D0%9A%D0%BE%D0%BD%D0%B4%D1%80%D0%B0%D1%82%D1%8C%D0%B5%D0%B2%D0%B0

[30] www.dgma.donetsk.ua/docs/doklad.ppt

[31] http://www.inion.ru/files/File/modernizaciya_Rossii_2013_Akaev_A_A.ppt 06.01.2014

Из схемы 1.3. отчетливо видно, что цивилизация входит в шестой цикл (длинную волну).

Схема 1.3.

Диффузия инноваций вдоль подъёмов циклов экономической активности Кондратьева

1.3.2. Интеллектуальные силы человека – основа шестого технологического уклада и сбой Бреттон-Вудской системы

Как уже отмечалось, цивилизация вошла в **шестой технологический уклад**. В отличие от предыдущих укладов**, в его основе не двигательная сила, направленная на базовые элементы глобальной конкуренции, а интеллектуальные силы человека.**

В течение четвертого и пятого технологических укладов глобальная конкуренция поддерживалась с помощью мощного финансового ресурса (долларов), исходящего, главным образом, из США и кредитующего многочисленных, главным образом, своих клиентов.

При переходе мировой экономики к шестому технологическому укладу происходит системный сбой, выражающийся в истощении и потенциала, и кредитного ресурса Бреттон-Вудской системы (позднее Ямайской валютной системы - свободной конвертации валют).

Этот сбой приводит к кризисным явлениям мировой финансовой системы и рынка инвестиций. В силу этого многие эксперты работают над её новой моделью, ориентированной на системные инновационные прорывы.

Это означает, что **в шестом технологическом укладе кредит как двигательная сила экономики (а точнее уже инфономики) уступает место интеллектуальной силе, направленной на конвергенцию высоких технологий (нано, био, информационных и когнитивных - NBIC-технологий).**[32]

1.3.3. Природа, предметы и действия, направленные на глобальную конкуренцию в шестом технологическом укладе

Природа, предметы и действия, направленные на глобальную конкуренцию в шестом технологическом укладе, исследуются рядом отечественных и зарубежных экспертов. Наиболее интересным представляется анализ В.В.Овчинникова, который частично приводится ниже (схема 1.4.)[33].

[32] Конструкция S (социо) + NBIC пока только обсуждается

[33] См.Овчинников В.В. Технологии глобальной конкуренции. М. ИНЭС-МАИБ. 2012. 280 с

Схема 1.4.

Здесь **предмет конкуренции характеризуется высоким уровнем конвергенции технологий в конструкциях NBIC и CCEIC**. **NBIC** - взаимопроникновение технологий с целью реализации сложнейших проектов, касающихся преобразования ресурсов в интеллектуальные силы в разных видах производственной деятельности. **CCEIC** - преобразование ресурсов в интеллектуальные силы для конвергенции облачных вычислений (CC - cloud computing), усиленных знаниями об экономической деятельности предприятия (E), моделировании генераторов отчетности (I) и когнитивных свойствах систем (C).

При этом владелец глобального индустриального центра сдает в аренду интеллектуальные оболочки, состоящие из платформ знаний, технологий и производства продукции. Одновременно он определяет предметы глобальной конкуренции (знания, технологии и производство инновационной продукции). С помощью интеллектуальных оболочек владелец подключается к инновационным и финансовым супер-

маркетам, обеспечивающим прозрачность, ответственность и высокое качество преобразования их ресурсов в интеллектуальные силы.

1.3.4. Шестой технологический уклад: новые возможности и стратегические риски для глобальной безопасности

С учетом появления принципиально новых вызовов и стратегических рисков для глобальной безопасности при переходе в шестой технологический уклад представляется оправданным привести **заявление Секретаря Совета Безопасности России Н.П.Патрушева от 4 июля 2013 г. «О четвертой международной встрече высоких представителей, курирующих вопросы безопасности»**, состоявшейся 2 - 4 июля 2013 года в г. Владивостоке.[34]

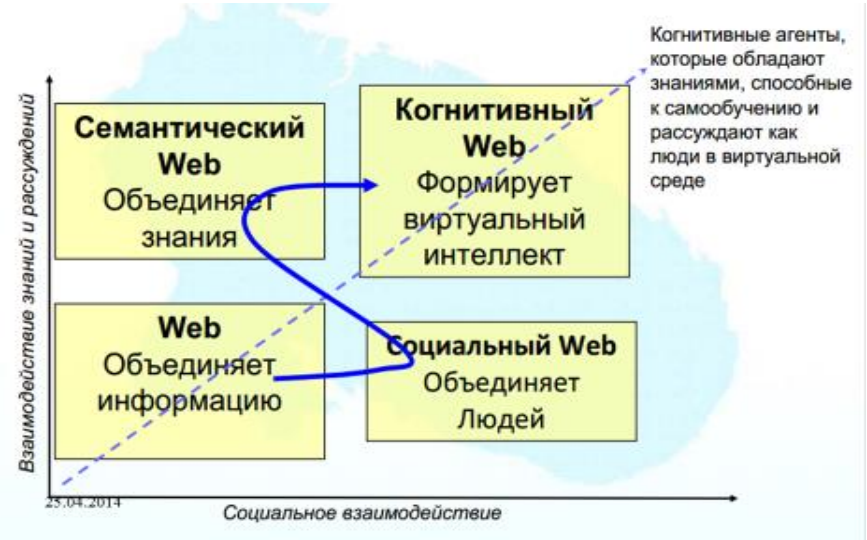
В работе четвертой международной встречи приняли участие делегации 60 стран, представляющие советы безопасности, аппараты президентов и глав правительств, министерств и ведомств, участвующих в выработке политики в области безопасности своих стран, а также руководство ООН.[35]

В заявлении Н.П.Патрушева было подчеркнуто, что в рамках четвертой международной встречи было «с интересом заслушано сообщение делегации Российской Федерации о современном этапе конвергенции наук и технологий как альтернативного ответа на новые вызовы и угрозы глобального характера. Подчеркивалась необходимость формирования нового эффективного международного механизма обеспечения безопасного развития и использования конвергентных технологий».

Эволюция когнитивных и web-технологий в контексте конвергенции НБИК-технологий может быть представлена следующей схемой 1.5.:

[34] http://www.scrf.gov.ru/news/794.html дата обращения 10.01.2014
[35] Пятая международная встреча намечена на 2014 г. в г.Казань.

Схема 1.5.



Одним из проектов подобных технологий является создание компьютера нового поколения мощностью квинтильон (10 в 18-й степени) вычислений в секунду Японским государственным исследовательским институтом Рикэн. Суперкомпьютер будет в 100 раз мощнее ныне существующей машины под названием «Кей», которая также принадлежит этому учреждению (занимает четвертое место в мировом рейтинге) и значительно превосходит лидера в этой области – «Тяньхэ-2», спроектированного Университетом оборонной науки и техники Народно-освободительной армии Китая.[36]

На проект планируется выделить 140 млрд. иен (около 1,37 млрд. долларов США) с завершением создания в 2020 г.

Самоочевидно, что, то государство, которое первым массово овладеет НБИК–технологиями, в т.ч. в военных целях, сможет диктовать свои правила игры в мировой политике.

[36] http://www.eurosmi.ru/772v_yaponii_sozdayut_kompyuter_novogo_pokoleniya.html 21.06.2014

Ничто не является хорошим или плохим.
Все зависит от того, как мы смотрим на вещи.

Уильям Шекспир

2. ГЕОПОЛИТИЧЕСКИЕ ВЫЗОВЫ ЦИФРОВОЙ ЭРЫ

2.1. Интегральная мощь ведущих стран мира

2.1.1. Базовые факторы стратегической матрицы государства

В рамках исследований, проводившихся Институтом экономических стратегий и Международной академией исследования будущего, была разработана методология и неоднократно решалась задача исследования глобального статуса государств с определением показателя их интегральной мощи[37].

[37] А.И.Агеев, Б.В.Куроедов и др. Глобальный рейтинг интегральной мощи 50 ведущих стран мира. М., Институт экономических стратегий, 2007 г.
А.И.Агеев, Б.В. Куроедов и др. Глобальный рейтинг интегральной мощи 100 ведущих стран мира. Доклад-2008 к обсуждению. 2-е издание, дополн. М.: Международная Академия исследований будущего, 2008 г.
А.И.Агеев, Б.В.Куроедов, О.В.Сандаров. Военный потенциал 100 ведущих стран мира. «Экономические стратегии», № 1, 2011 г.
А.И.Агеев, Б.В.Куроедов и др. Глобальный рейтинг интегральной мощи 100 ведущих стран мира. Доклад-2012 к обсуждению. 3-е издание, переработ, и дополн. М.: Международная Академия исследований будущего, Институт экономических стратегий, 2012.
全 球百强综合国力排行榜 100 2012年全球100个国家综合实力排行榜
关于此次2012年讨论报
告 第三版莫斯科 2012年 (Глобальный рейтинг интегральной мощи
на китайском языке).
A.Ageev, B.Kuroedov. «Global Rating of Integral Power of 100 World's Leading Countries. Report-2012 to be discussed. 3rd edition, revised and enlarged».M: International Futures Research Academy, Institute for Economic Strategies, 2012.
Подробнее на сайте www.ks-forecastclub.ru

Оценка статуса и прогнозной динамики процесса государственного развития осуществляется в модели стратегической матрицы по девяти базовым факторам (рис. 2.1).

Рис. 2.1. Базовые факторы
стратегической матрицы государства

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»[38].

Конечным интегральным показателем помимо значений девяти базовых факторов выступает интегральный показатель мощи (ИПМ) государства, позволяющий обобщить полученные значения девяти факторов государственной мощи[39].

---

[38] А.И.Агеев, Б.В.Куроедов, Р.Мэтьюз, О.В.Сандаров. Методология стратегической матрицы. М., Институт экономических стратегий, 2004 г.

[39] «Понятия **«потенциал»** и **«мощь»** по своему содержанию не идентичны, поскольку они соответствуют философским категориям действительности и возможности. Как действительность представляет собой реализацию существующих потенций бытия и практики как его социальной формы, так и мощь есть степень реализации потенциала при данных (объективных и субъективных) условиях. Полная реализация совокупного потенциала государства, как отмечалось, происходит далеко не всегда, хотя максимально возможным уровнем сово-

2.1.2. Россия, ЕС, Китай и США в мировом интегральном рейтинге

На основе оценки 2012 г. Россия, ЕС, Китай и США возглавили первую четверку глобального рейтинга 100 ведущих государств мира (табл. 1, рис. 2.2. – 2.10.).

Россия по рейтингу ИПМ (6 баллов) занимает четвертое место в мире. По абсолютному значению ИПМ идущий на третьем месте Китай (7,3 балла) существенно опережает Россию. Европейский союз, рассматриваемый как единое целое, занимает вторую позицию мирового рейтинга с результатом ИПМ = 7,7 балла, достигнув статуса сверхдержавы и уступая лишь США (ИПМ = 8,1 балла). При этом по отдельным показателям («Население», «Культура и религия») ЕС превосходит США.

купной мощи государства и является этот потенциал. Фактически совокупный потенциал государства, как категория возможности, представляет собой более широкое, но менее конкретное понятие, чем совокупная мощь государства, которая, как категория действительности, обладает конкретной совокупностью реализованных факторов и условий как объективного, так и субъективного характера».
Прохожев А.А. Общая теория национальной безопасности. Учебник. М.,РАГС, 2005.

Таблица 1. Значения интегрального показателя мощи (ИПМ) для ЕС, Китая, России и США и их рейтинг в ряду 100 ведущих государств мира.

Страна	Управление	Территория	Природные ресурсы	Население	Экономика	Культура и религия	Наука и образование	Армия	Геополити-ческое положение	Интегра-льный показатель мощи	Место в Рейтинге - 2012
Коэффициент важности (Mi)	0,14	0,09	0,09	0,14	0,18	0,05	0,09	0,14	0,09		
Россия	5,1	10,0	8,4	3,6	5,1	6,0	5,0	7,5	5,0	6,00	1
ЕС	6,4	7,8	6,9	6,7	7,8	9,0	8,0	7,8	8,5	7,67	2
Китай	7,1	8,7	7,3	8,6	7,0	8,0	5,0	7,3	7,0	7,32	3
США	6,9	8,8	8,9	5,8	7,6	8,0	8,5	9,7	9,5	8,14	4

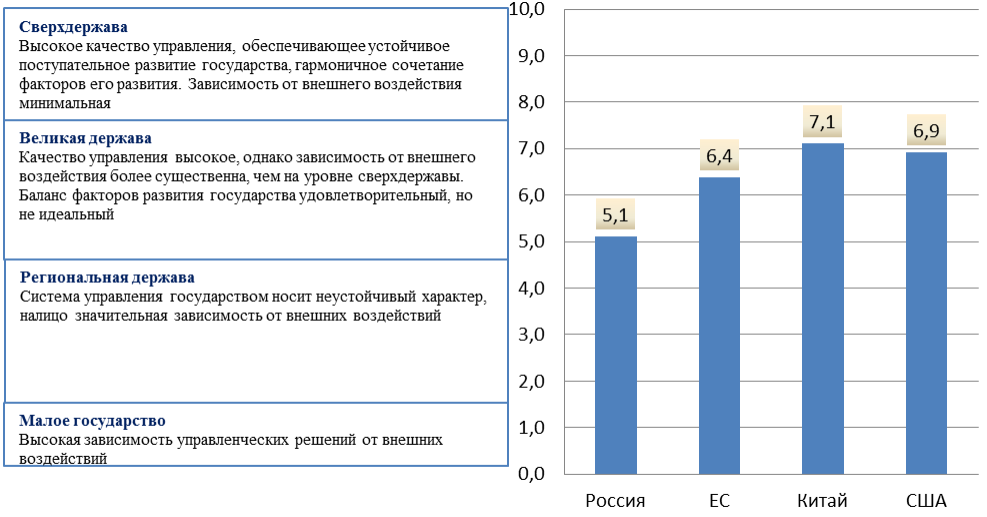


Рис. 2.2. Значения показателя «Управление» для России, ЕС, Китая и США

Сверхдержава
Государство, обеспечивающее развитие национальной экономики за счет собственных природных ресурсов на 80—100%. Благоприятные природно-климатические условия.

Великая держава
Обеспеченность экономики собственными ресурсами - 50-80%. Хорошие природно-климатические условия.

Региональная держава
Обеспеченность экономики собственными ресурсами - 30-50%. Удовлетворительные природно-климатические условия.

Малое государство
Обеспеченность ресурсами ниже 30%

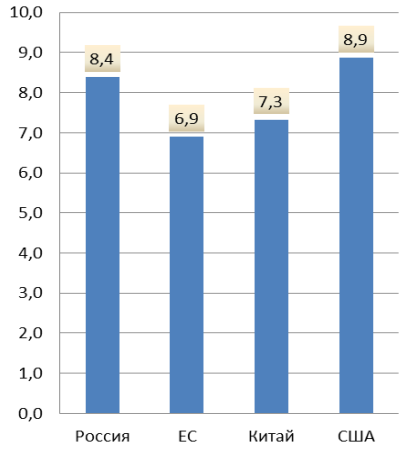


Рис. 2.3. Значения показателя «Природные ресурсы» для России, ЕС, Китая и США

Сверхдержава
от 300 млн. до более чем 1 млрд.чел.
высокий уровень жизни и образования

Великая держава
120-300 млн.чел.
уровень жизни и образовани выше среднего

Региональная держава
30-120 млн.чел.
средний уровень жизни и образования

Малое государство
Менее 30 млн.чел.

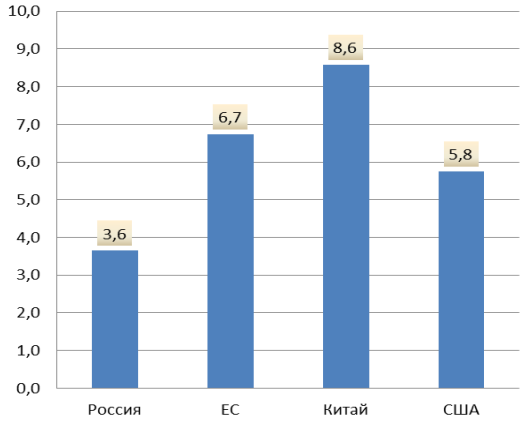


Рис. 2.4. Значения показателя «Население» для России, ЕС, Китая и США

Сверхдержава
Государство, развитие экономики которого играет определяющую роль для развития мировой экономики
ВВП по паритету покупательной способности более 10000 млрд долл.

Великая держава
Государство, чья экономика в состоянии оказывать существенное воздействие на развитие мировой экономики, в том числе в отдельных ее секторах
ВВП по паритету покупательной способности 1500-10000 млрд долл.

Региональная держава
Экономика государства не является ключевым элементом общемировой системы, но оказывает заметное воздействие на жизнь региона
ВВП по паритету покупательной способности 150-1500 млрд долл.

Малое государство
Малозначимая экономика. ВВП по паритету покупательной способности менее 150 млрд долл.

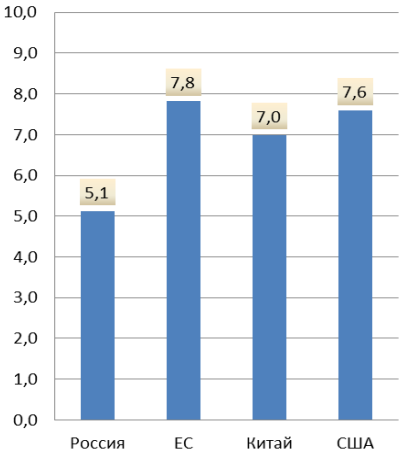


Рис. 2.5. Значения показателя «Экономика»
для России, ЕС, Китая и США

Сверхдержава
Страна является самобытной цивилизацией, ее культура определяет общемировые тенденции развития. Достижения культуры признаны во всем мире, является центром одной из мировых религий.

Великая держава
Страна развивает культуру, в отдельных областях оказывает заметное воздействие на формирование мировой культуры. Религия имеет мировое значение.

Региональная держава
Страна обладает самобытной, устойчивой к внешним воздействиям культурой, религия влиятельна в региональном масштабе.

Малое государство
Культура имеет локальное, «этнографическое» значение

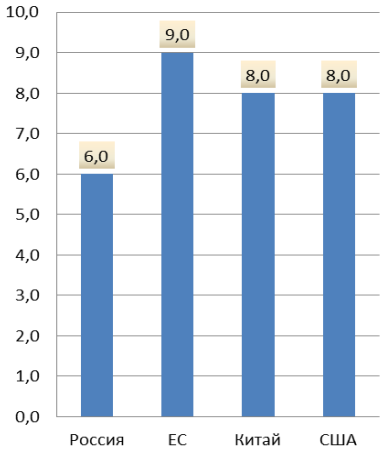


Рис. 2.6. Значения показателя «Культура и религия»
для России, ЕС, Китая и США

Рис. 2.7. Значения показателя «Наука и образование» для России, ЕС, Китая и США

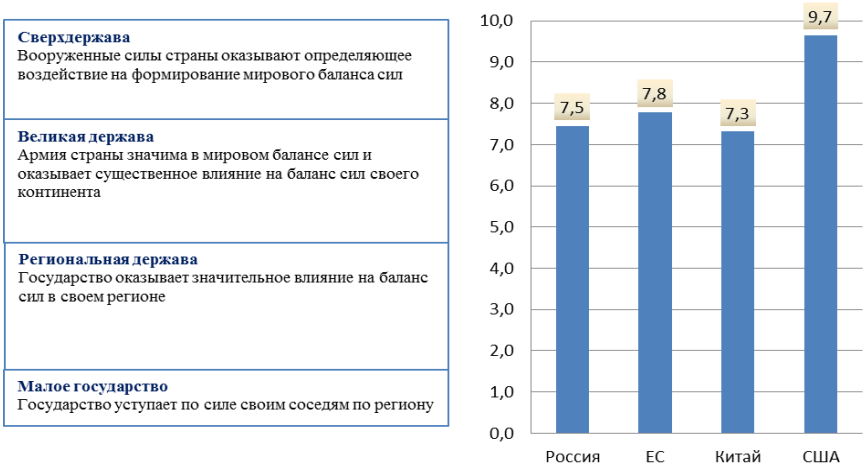


Рис. 2.8. Значения показателя «Армия» для России, ЕС, Китая и США

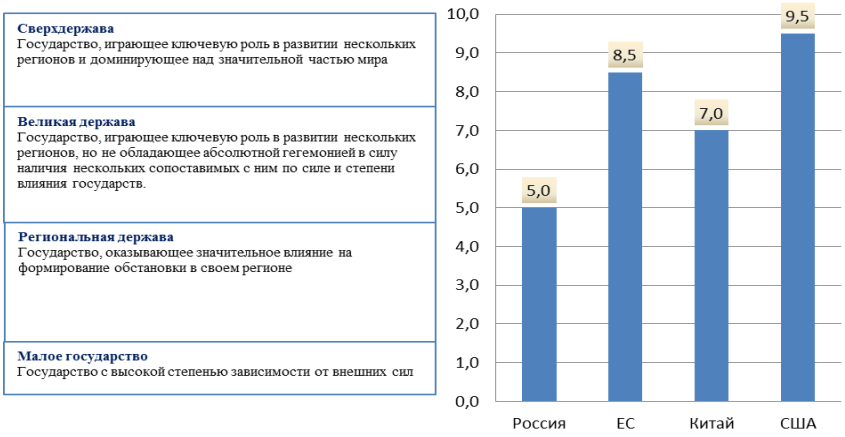
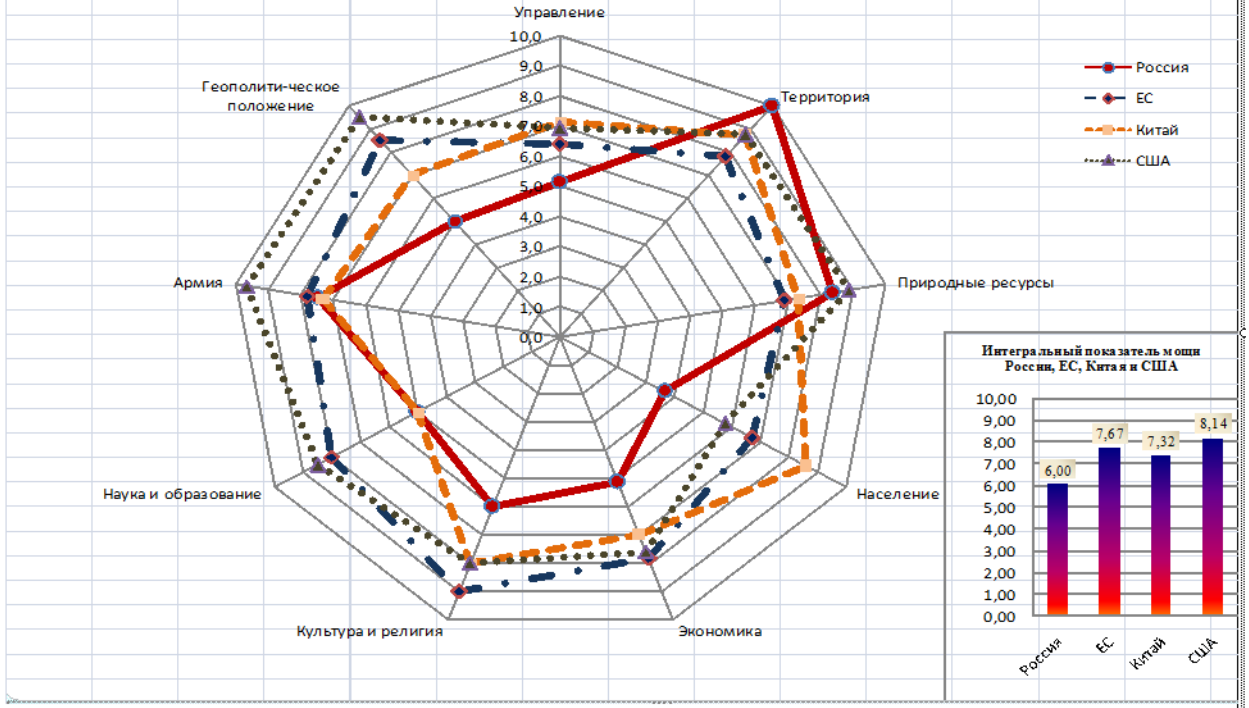


Рис. 2.9. Значения показателя «Внешняя политика» для России, ЕС, Китая и США

Рис. 2.10. Основные показатели мощи России, ЕС, Китая и США



2.2. Методология оценки сетевой мощи государства

В отличие от решения задачи по исследованию глобального статуса государств и определению показателя их интегральной мощи изучение их сетевой мощи в большей мере базируется на оценке реализации имеющегося у страны потенциала, фактически его конвертации в степень глобального влияния, задействуемого для обеспечения национальных интересов.

Представляется, что, хотя собственно сетевое могущество государства определяется синергетическим эффектом в результате реализации его потенциальных возможностей, общая оценка сетевой мощи может быть осуществлена через ее проявление в четырех основных сферах: политической, военной, экономической и информационной (рис. 2.11.).

Рис. 2.11. Сферы проявления сетевой мощи

Для того, чтобы иметь возможность сопоставления и обобщения этих оценок, представляется целесообразным сформировать 10-бальные оценочные шкалы, которые на ос-

нове ранее заявленного подхода будут определять верхний, средний и нижний уровни влияния государства в диапазонах «сверхдержава», «великая держава», «региональная держава» и низший уровень – «малое государство».

Для формирования этой шкалы используются несколько градаций категорий превосходства, значимости и участия в формировании баланса (табл. 2).

Табл.2. Шкала оценки влияния

Категория страны	Баллы	Оценка влияния
Сверхдержава	10	Явное
	9	**Превосходство**
	8	Неявное
Великая держава	7	Явная
	6	**Значимость**
	5	Неявная
Региональная держава	4	Явное
	3	**Участие**
	2	Неявное
Малое государство	1	Незначительное

Для оценки политического, военного, экономического и, в несколько меньшей степени, информационного влияния важным представляется оценить глобальную степень влияния государства через оценки его значимости в отдельных регионах мира, а для военной составляющей и на океанских и морских театрах. При этом регионы различаются по степени их значимости для глобального баланса влияния, которая оценивается на основе экспертных мнений путем их ранжирования с последующим расчетом коэффициента геополитической важности (Gi) на основе метода дробей Фишберна, который представлен формулой (1):

$$G_i = \frac{\max(V_n) - V_i + 1}{\sum V_i}$$, i, *n*=1,N , (1),

где:

G_i – весовой коэффициент геополитической значимости i-го региона,

V_i – определяемый экспертом ранг важности i-го региона,

$\max(V_n)$ – максимальное (т.е. наихудшее) значение ранга важности

N – общее количество рассматриваемых регионов

Оценка глобального влияния в соответствующей сфере рассчитывается по формуле (2):

$$Ws = \sum_{i=1,l} Gi * Zi \qquad (2)$$

где

Ws - значение уровня глобального влияния в рассматриваемой сфере

l – количество оцениваемых частных параметров;

Gi – весовой коэффициент геополитической значимости i-го региона,

Zi – экспертная оценка влияния государства в избранной сфере для i-го региона в баллах.

Сетевая мощь, как на региональном, так и на глобальном уровне определяется как среднеарифметическое значение соответствующих оценок в различных сферах на основе допущения о том, что их важность друг относительно друга приблизительно равна.

В противном случае может быть задействован алгоритм расчета аналогичный тому, который описывается формулами 1 и 2.

2.3. Оценка текущего статуса сетевой мощи России, ЕС, Китая и США

Используя представленную выше методику, были произведены расчеты текущей сетевой мощи России, ЕС, Китая и США, результаты которого представлены в табл. 3 - 6.

Оценки России, как в отдельных сферах, так и по уровню сетевой мощи концентрируются вокруг значения в 6 баллов, что соответствует среднему уровню сверхдержавы (рис. 2.12., 2.13.). Несколько неожиданно наиболее высоко оценено политическое влияние (6,2 балла). В 5,8 балла оценено информационное влияние. Наиболее низкие оценки получили показатели экономического (5,4 балла) и военного (5,6 балла) влияния.

Оценки политического и информационного влияния не в последнюю очередь вытекают, видимо, из статуса России как постоянного члена Совета безопасности ООН и ее политике по противодействию стремлению Запада к превращению Организации Объединённых Наций и системы международного права в инструменты обслуживания исключительно интересов западного сообщества. Кроме того, продолжающаяся геополитическая и экономическая экспансия Запада на постсоветском пространстве, препятствующая успеху евразийских интеграционных процессов, объективно заставляет Россию занимать активную внешнеполитическую позицию и существовать в условиях достаточно жесткой, в том числе и информационной, конфронтации.

Невысокое значение экономического влияния вполне объяснимо слабым присутствием России на рынках высокотехнологичной продукции и преобладанием сырьевых ресурсов в структуре российского экспорта.

Хотя, благодаря своему ядерному потенциалу, Россия и остается № 3 в мировой военной иерархии (см. п.2.1.2.), ее геополитическая зажатость между НАТО (США № 1 и ЕС № 2 глобального военного баланса) и Китаем (№ 4 военного

рейтинга) объясняют слабую конвертацию ее военного потенциала в уровень глобального влияния.

Европейский союз еще не закончил процесс собственного становления, но во все в большей мере может рассматриваться в качестве единого государственного образования. По большинству параметров (политическое влияние – 7,1 балла; экономическое – 7,3; информационное – 6,7; сетевая мощь – 6,8) ЕС вплотную подбирается к уровню «свердержавы». При этом просматривается тенденция к некоторому самоограничению в конвертации имеющегося потенциала в уровень влияния, когда по многим вопросам ЕС не стремится занять обособленную позицию, а выступает ведомым на платформе евроатлантической солидарности с претендующими на единоличное мировое лидерство США.

Хотя отмечается рост военной активности отдельных членов ЕС (прежде всего, Франции), уровень военного влияния ЕС оценивается относительно невысоко (5,9 балла), что, скорее всего, характеризует уже упомянутую зависимость в сфере военно-политических решений от позиции США.

Китай значительно превосходит Россию по большинству оценок влияния (6,6 баллов в политической, 7,6 в экономической, 6,2 в информационной сфере) и сетевой мощи (6,4 балла), однако несколько уступает в оценке военного влияния (5,2 балла). При этом структура его сетевого влияния (рис. 2.13.) удивительным образом почти совпадает с параметрами Евросоюза.

Занимая во многом сходные с Россией позиции в вопросах мироустройства, Китай умудряется в меньшей степени открыто конфликтовать с западным миром. Это, не в последнюю очередь, базируется на его более высоком экономическим статусе важнейшего торгового партнера США и ЕС, что объясняет явное нежелание Запада чрезмерно обострять отношения.

Относительно невысокая оценка военного влияния Китая объясняется его сосредоточенностью на формировании бла-

гоприятного для него военного баланса в Северо-Восточной Азии и прилегающих акваториях Восточно-Китайского и Южно-Китайского морей. Кроме того, очевидно, что увеличения своего геополитического веса в мире на данном этапе Китай стремится достичь преимущественно за счет расширения сфер экономического влияния.

Оценка сетевого влияния США (8,1 балла) и структура этого влияния (политическая сфера – 8,1; экономическая – 7,7; информационная – 8,1; военная – 8,7) подтверждают тезис о том, что с развалом СССР США утвердились в статусе единственной полноценной сверхдержавы современного мира.

Интересно отметить, что по степени экономического влияния ЕС и Китай практически сравнялись с США, а вот по военному влиянию США, несомненно, намного опережают любого из ближайших конкурентов.

Табл.3. Оценка сетевой мощи России в регионах (океанах) мира

Регионы и океаны	Геополитическая значимость региона (Gi)	Политическое влияние	Экономическое влияние	Информационное влияние	Геополитическая значимость региона (Gi)	Военное влияние	Сетевая мощь
Западная Европа	0,11	7	6	6	0,08	7	6,50
Центральная и Восточная Европа	0,11	7	7	6	0,08	7	6,75
Ближний и Средний Восток	0,11	6	5	6	0,08	5	5,50
Центральная Азия	0,08	8	8	7	0,06	8	7,75
Южная Азия	0,06	6	6	6	0,04	4	5,50
Северо-Восточная Азия	0,11	7	7	7	0,08	7	7,00
Юго-Восточная Азия	0,08	5	4	5	0,06	4	4,50
Северная Африка	0,08	5	5	5	0,06	3	4,50
Африка южнее Сахары	0,03	5	5	4	0,02	3	4,25
Австралия и Океания	0,03	3	3	3	0,02	2	2,75
Северная Америка	0,11	6	3	6	0,08	7	5,50
Центральная и Южная Америка	0,08	6	4	5	0,06	2	4,25
Атлантический океан					0,08	7	
Северный Ледовитый океан					0,06	7	
Тихий океан					0,08	7	
Индийский океан					0,08	3	
Глобальная оценка		**6,22**	**5,42**	**5,81**		**5,59**	**5,76**

Табл.4. Оценка сетевой мощи ЕС в регионах (океанах) мира

Регионы и океаны	Геополитическая значимость региона (Gi)	Политическое влияние	Экономическое влияние	Информационное влияние	Геополитическая значимость региона (Gi)	Военное влияние	Сетевая мощь
Западная Европа	0,11	9	9	8	0,08	9	8,75
Центральная и Восточная Европа	0,11	8	8	8	0,08	9	8,25
Ближний и Средний Восток	0,11	7	8	7	0,08	7	7,25
Центральная Азия	0,08	6	7	6	0,06	4	5,75
Южная Азия	0,06	6	7	7	0,04	4	6,00
Северо-Восточная Азия	0,11	6	7	7	0,08	4	6,00
Юго-Восточная Азия	0,08	7	7	6	0,06	4	6,00
Северная Африка	0,08	8	7	7	0,06	7	7,25
Африка южнее Сахары	0,03	7	7	6	0,02	7	6,75
Австралия и Океания	0,03	6	6	6	0,02	3	5,25
Северная Америка	0,11	7	7	6	0,08	7	6,75
Центральная и Южная Америка	0,08	6	6	5	0,06	5	5,50
Атлантический океан					0,08	8	
Северный ледовитый океан					0,06	7	
Тихий океан					0,08	3	
Индийский океан					0,08	4	
Глобальная оценка		**7,06**	**7,33**	**6,72**		**5,94**	**6,76**

Табл.5. Оценка сетевой мощи Китая в регионах (океанах) мира

Регионы и океаны	Геополитическая значимость региона (Gi)	Политическое влияние	Экономическое влияние	Информационное влияние	Геополитическая значимость региона (Gi)	Военное влияние	Сетевая мощь
Западная Европа	0,11	6	8	5	0,08	5	6,00
Центральная и Восточная Европа	0,11	5	7	5	0,08	5	5,50
Ближний и Средний Восток	0,11	6	7	5	0,08	4	5,50
Центральная Азия	0,08	7	8	7	0,06	8	7,50
Южная Азия	0,06	7	7	6	0,04	8	7,00
Северо-Восточная Азия	0,11	8	9	9	0,08	8	8,50
Юго-Восточная Азия	0,08	8	9	7	0,06	8	8,00
Северная Африка	0,08	6	7	5	0,06	3	5,25
Африка южнее Сахары	0,03	8	8	7	0,02	4	6,75
Австралия и Океания	0,03	7	7	7	0,02	6	6,75
Северная Америка	0,11	7	7	7	0,08	7	7,00
Центральная и Южная Америка	0,08	6	7	5	0,06	2	5,00
Атлантический океан					0,08	1	
Северный ледовитый океан					0,06	1	
Тихий океан					0,08	7	
Индийский океан					0,08	6	
Глобальная оценка		**6,61**	**7,61**	**6,17**		**5,18**	**6,39**

Табл.6. Оценка сетевой мощи США в регионах (океанах) мира

Регионы и океаны	Геополитическая значимость региона (Gi)	Политическое влияние	Экономическое влияние	Информационное влияние	Геополитическая значимость региона (Gi)	Военное влияние	Сетевая мощь
Западная Европа	0,11	8	8	9	0,08	9	8,50
Центральная и Восточная Европа	0,11	9	7	9	0,08	9	8,50
Ближний и Средний Восток	0,11	8	8	7	0,08	8	7,75
Центральная Азия	0,08	7	7	7	0,06	7	7,00
Южная Азия	0,06	7	7	7	0,04	7	7,00
Северо-Восточная Азия	0,11	8	7	8	0,08	8	7,75
Юго-Восточная Азия	0,08	8	7	8	0,06	8	7,75
Северная Африка	0,08	8	7	7	0,06	9	7,75
Африка южнее Сахары	0,03	7	7	6	0,02	7	6,75
Австралия и Океания	0,03	9	6	9	0,02	10	8,50
Северная Америка	0,11	10	10	10	0,08	10	10,00
Центральная и Южная Америка	0,08	7	9	8	0,06	9	8,25
Атлантический океан					0,08	9	
Северный ледовитый океан					0,06	8	
Тихий океан					0,08	9	
Индийский океан					0,08	10	
Глобальная оценка		**8,11**	**7,69**	**8,08**		**8,67**	**8,14**

Рис. 2.12. Структура сетевого влияния

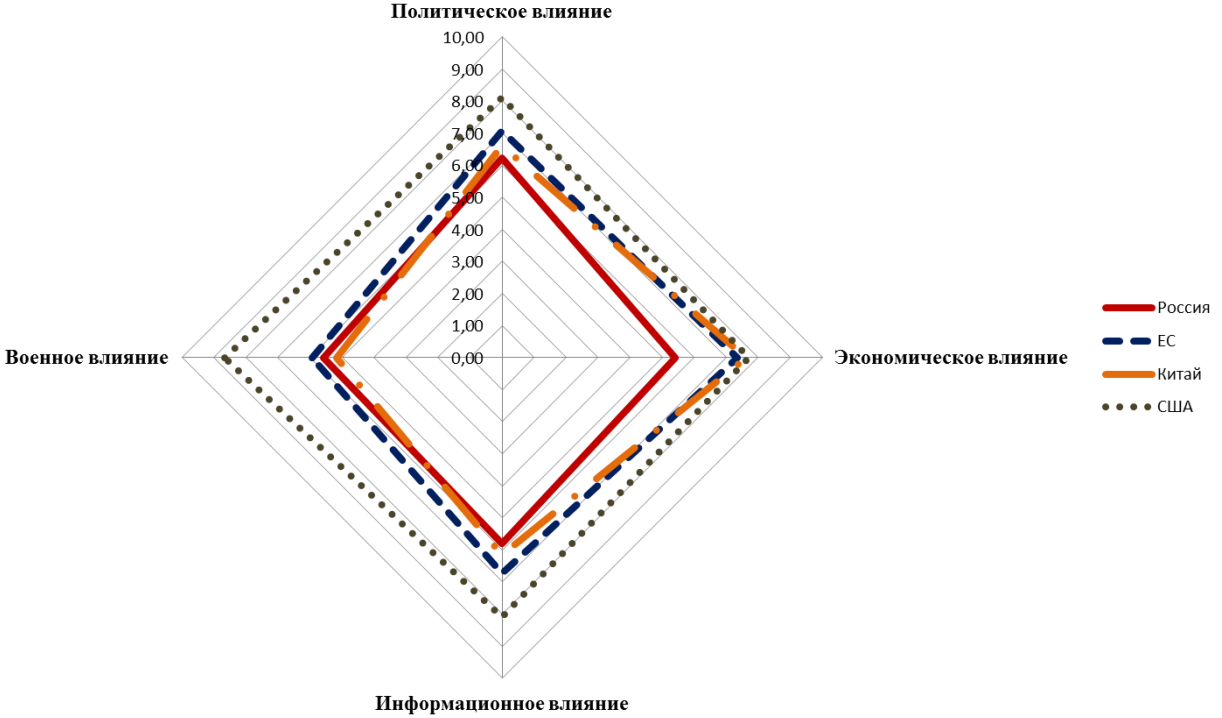
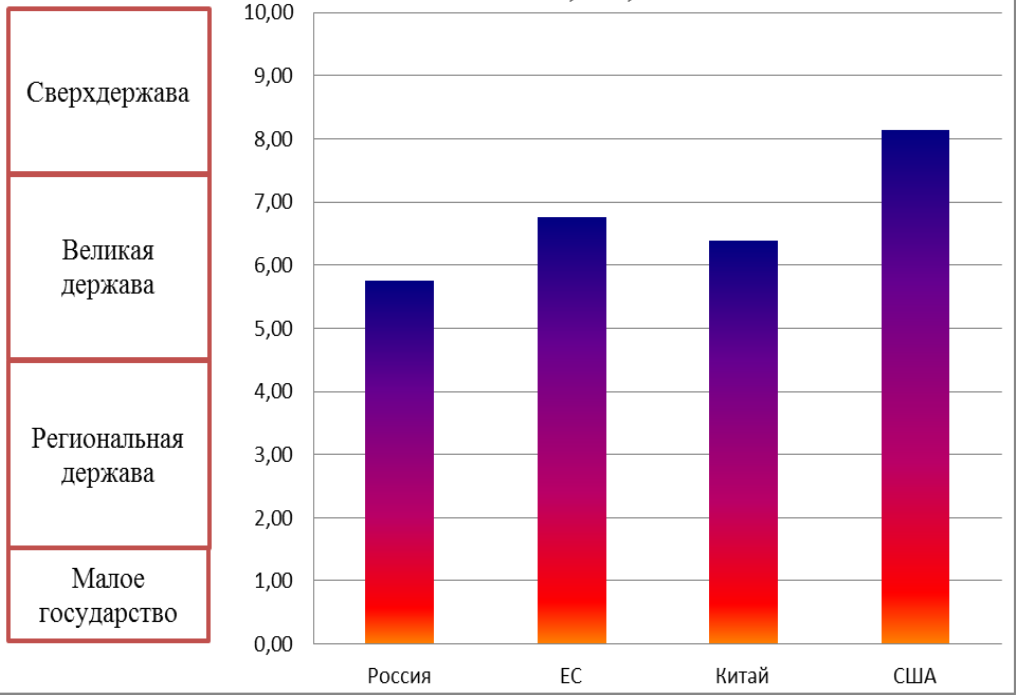


Рис. 2.13. Сетевая мошь России. ЕС. Китая и США



2.3.1. Прогноз изменения баланса сетевой мощи

Ключевым вопросом при прогнозе изменения сетевого влияния субъектов международной деятельности в обозримой перспективе является возможность их укрупнения за счет интеграционных процессов различного уровня.

Так, формирование зоны свободной торговли между ЕС и США может вывести на новый уровень отношения трансатлантического партнерства. Отмена таможенных пошлин и снятие торговых ограничений позволят усилить экономическую составляющую отношений США и ЕС, которые в военной и политической сфере тесно координируют свои действия на уровне институтов НАТО и не только. При дальнейшем развитии этих процессов может возникнуть интеграционное объединение государств, на которые ныне приходятся примерно половина мирового ВВП и треть глобальной торговли. Попытка оценить возможные значения сетевой мощи подобного субъекта международных отношений представлена в табл. 7.

Подобный субъект обладал бы очень гармоничной структурой сетевого влияния (по 8,7 балла – политическое, экономическое и информационное влияние; 9 баллов военное влияние) общая оценка составила бы величину 8,9 балла, т.е. практически - мировая гегемония.

Россия в последнее время активизировала усилия по интеграции Евразийского пространства, однако окончательная конфигурация возможного интеграционного объединения станет ясной в начале 2015 г. (подробнее этот вопрос освещен в ряде других работ[40]).

[40] А.И.Агеев, И.В. Бестужев-Лада, Б.В.Куроедов и др. Россия и мир: взгляд из 2017 года. М., Институт экономических стратегий, 2007 г.
А.И.Агеев, Б.В.Куроедов, О.В.Сандаров. Глобальная безопасность: инновационные методы анализа конфликтов (под общей редакцией А.И. Смирнова). Раздел 4.4. Информационно-аналитические комплексы Института экономических стратегий (ИНЭС). М., Общество «Знание» России, 2011 г. (http://www.ks-forecastclub.ru/publications.html)

Однако если взять за основу некий усредненный вариант для Евразийского интеграционного объединения, то примерные значения его сетевой мощи могут составить: в политической сфере – 6,5 балла, в экономической сфере – 6 баллов, в информационной 6,4 балла, в военной – 5,7. Совокупная сетевая мощь для этого варианта составит 6,1 балла.

Возможное приращение сетевой мощи за счет евразийской интеграции на глобальном и региональных уровнях по отношению текущему статусу России можно проследить на рис. 2.14.

Гипотетически можно рассмотреть также вариант наращивания интеграционных усилий в формате Шанхайской организации сотрудничества (ШОС) и присоединение к этому процессу ряда сильных региональных стран, например, Ирана. Теоретически, это позволило бы создать объединение государств с характеристиками сетевого влияния на уровне: в политической сфере – 7,3 балла, в экономической сфере – 7,7 баллов, в информационной 7,1 балла, в военной – 6,7 балла. Совокупная сетевая мощь для этого варианта составит 7,2 балла (табл. 9).

И Евразийскому союзу, и гипотетическому интеграционному объединению в расширенном формате ШОС трудно соперничать с объединением США и ЕС по характеристикам своей сетевой мощи (рис. 2.15.) на глобальном уровне. Однако реализация этих проектов может стать для стран-участниц достаточным условием обеспечения устойчивого и стабильного развития в рамках нескольких регионов Евразии и компенсации деструктивных внешних воздействий.

Табл.7. Оценка сетевой мощи "Евроатлантической оси" в регионах (океанах) мира

Регионы и океаны	Геополитическая значимость региона (Gi)	Политическое влияние	Экономическое влияние	Информационное влияние	Геополитическая значимость региона (Gi)	Военное влияние	Сетевая мощь
Западная Европа	0,11	10	10	10	0,08	10	10,00
Центральная и Восточная Европа	0,11	10	10	10	0,08	10	10,00
Ближний и Средний Восток	0,11	9	9	9	0,08	10	9,25
Центральная Азия	0,08	7	7	7	0,06	7	7,00
Южная Азия	0,06	8	8	7	0,04	8	7,75
Северо-Восточная Азия	0,11	8	7	8	0,08	8	7,75
Юго-Восточная Азия	0,08	8	8	8	0,06	8	8,00
Северная Африка	0,08	8	9	9	0,06	9	8,75
Африка южнее Сахары	0,03	8	8	8	0,02	7	7,75
Австралия и Океания	0,03	9	8	9	0,02	10	9,00
Северная Америка	0,11	10	10	10	0,08	10	10,00
Центральная и Южная Америка	0,08	8	9	8	0,06	9	8,50
Атлантический океан					0,08	9	
Северный ледовитый океан					0,06	8	
Тихий океан					0,08	9	
Индийский океан					0,08	10	
Глобальная оценка		**8,72**	**8,75**	**8,75**		**9,02**	**8,81**

Табл.8. Оценка сетевой мощи "Евразийского союза" в регионах (океанах) мира

Регионы и океаны	Геополитическая значимость региона (Gi)	Политическое влияние	Экономическое влияние	Информационное влияние	Геополитическая значимость региона (Gi)	Военное влияние	Сетевая мощь
Западная Европа	0,11	7	6	6	0,08	7	6,50
Центральная и Восточная Европа	0,11	7	7	7	0,08	7	7,00
Ближний и Средний Восток	0,11	7	7	7	0,08	5	6,50
Центральная Азия	0,08	9	9	9	0,06	9	9,00
Южная Азия	0,06	7	7	7	0,04	5	6,50
Северо-Восточная Азия	0,11	7	7	7	0,08	7	7,00
Юго-Восточная Азия	0,08	5	5	6	0,06	4	5,00
Северная Африка	0,08	5	5	5	0,06	3	4,50
Африка южнее Сахары	0,03	5	5	5	0,02	3	4,50
Австралия и Океания	0,03	3	3	3	0,02	2	2,75
Северная Америка	0,11	6	3	6	0,08	7	5,50
Центральная и Южная Америка	0,08	6	5	6	0,06	2	4,75
Атлантический океан					0,08	7	
Северный ледовитый океан					0,06	7	
Тихий океан					0,08	7	
Индийский океан					0,08	3	
Глобальная оценка		**6,47**	**5,94**	**6,44**		**5,69**	**6,14**

Табл.9. Оценка сетевой мощи «ШОС+Иран» в регионах (океанах) мира

Регионы и океаны	Геополитическая значимость региона (Gi)	Политическое влияние	Экономическое влияние	Информационное влияние	Геополитическая значимость региона (Gi)	Военное влияние	Сетевая мощь
Западная Европа	0,11	7	8	6	0,08	7	7,00
Центральная и Восточная Европа	0,11	7	7	7	0,08	7	7,00
Ближний и Средний Восток	0,11	7	7	7	0,08	5	6,50
Центральная Азия	0,08	9	9	9	0,06	9	9,00
Южная Азия	0,06	7	7	7	0,04	8	7,25
Северо-Восточная Азия	0,11	8	9	8	0,08	9	8,50
Юго-Восточная Азия	0,08	8	9	7	0,06	8	8,00
Северная Африка	0,08	6	7	6	0,06	3	5,50
Африка южнее Сахары	0,03	7	8	7	0,02	3	6,25
Австралия и Океания	0,03	7	7	7	0,02	6	6,75
Северная Америка	0,11	7	7	7	0,08	7	7,00
Центральная и Южная Америка	0,08	7	7	7	0,06	4	6,25
Атлантический океан					0,08	7	
Северный ледовитый океан					0,06	7	
Тихий океан					0,08	7	
Индийский океан					0,08	7	
Глобальная оценка		**7,28**	**7,69**	**7,08**		**6,71**	**7,19**

Рис. 2.14. Сопоставление сетевой мощи России и гипотетических интеграционных объединений

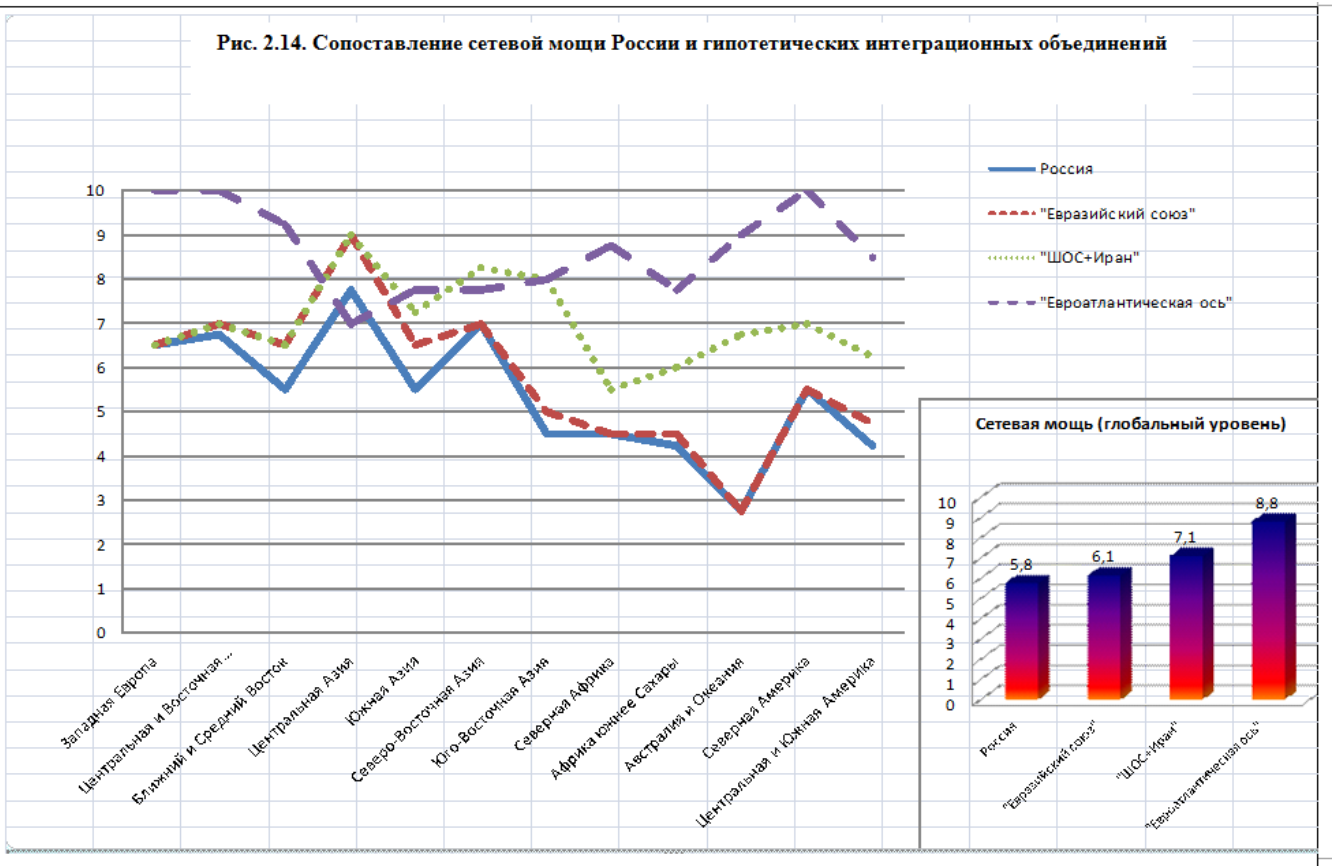
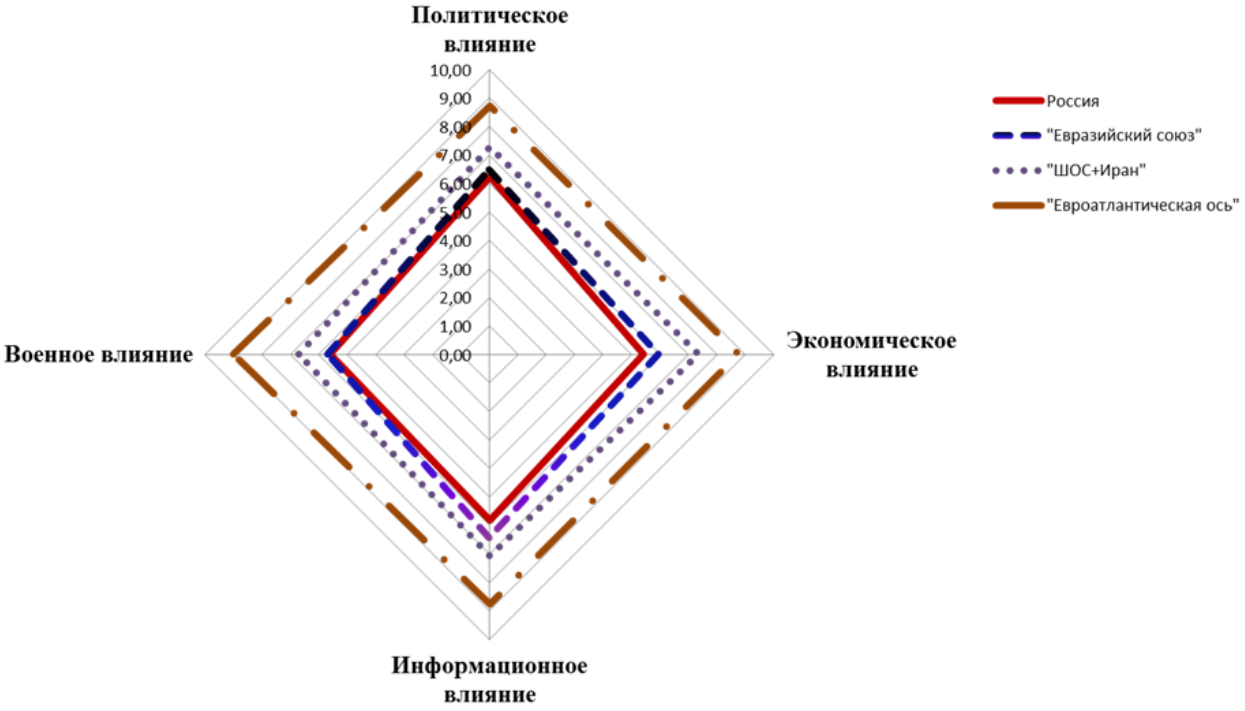


Рис. 2.15. Возможная структура сетевой мощи интеграционных объединений в сравнении с показателями России



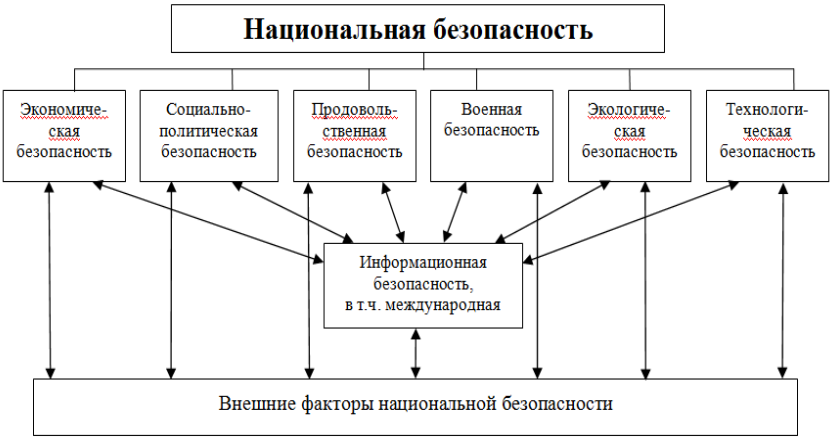
3. УКРЕПЛЕНИЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (МИБ) КАК МЕГАТРЕНД СОВРЕМЕННОЙ МИРОВОЙ ПОЛИТИКИ

Как уже отмечалось, планета охвачена беспрецедентной информационной революцией. Её феномен создал условия для формирования глобальной информационной инфраструктуры, которая предоставила принципиально новые возможности социализации людей, их общения и доступа к накопленным человечеством знаниям.

Однако ИКТ, будучи технологиями двойного назначения, стали не только локомотивом, но и нервом глобализации, ибо несут в себе принципиально новые вызовы и стратегические риски.

Действительно, информационная безопасность пронизывает практически все составляющие национальной безопасности (схема 3.1.).

Схема 3.1.



Одновременно 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 мира.

3.1. Дискурс МИБ в ООН

3.1.1. Россия – инициатор и локомотив продвижения МИБ

Мощным импульсом к поиску решения проблемы МИБ стала появившаяся в конце 1990-х годов информация контрольно-финансового управления Конгресса США о том, что около 120 стран разрабатывают оружие шестого поколения – информационное (в то время как разработку ядерного оружия осуществляют не более 20)[41].

Особую актуальность данной проблематике придавала способность ИКТ 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.

Таким образом, **проблематика МИБ трансформировалась из технологической в военно-политическую и стала одним из ключевых мегатрендов мировой политики.**

В силу этого Россия инициативно поставила вопрос об обеспечении МИБ в ООН: 23 сентября 1998 г. Генсекретарю ООН было направлено специальное Послание по проблеме

[41] См. А. В. Крутских. Война или мир: международные аспекты информационной безопасности //Статья из сборника "Научные и методологические проблемы информационной безопасности" (под ред. В. П. Шерстюка, М., МЦНМО, 2004 г.)

МИБ Министра иностранных дел России И.С.Иванова.[42] Важнейшей задачей ставилось 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. (Позднее эта позиция нашла отражение и развитие 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.), госпрограмме «Информационное общество (2011-2020 гг.) от 20 октября 2010 г., а также в Концепции внешней политики России (2013 г.)).

Предложенная Россией в 1998 г. резолюция Генассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» была принята консенсусом (с некоторыми поправками)[43]. Резолюция призывала к рассмотрению существующих и потенциальных угроз в сфере информбезопасности, определению основных понятий, оценке целесообразности разработки соответствующих международных принципов. В принятом в 1999 г. ГА ООН обновленном проекте данной резолюции № 54/49 впервые была сформулирована «триада угроз» в сфере МИБ: применение ИКТ в военных, террористических и преступных целях.

---

[42] См. А.В.Крутских, Н.В.Соколова. Проблема обеспечения международной информационной безопасности: современный этап. Дипломатический ежегодник - 2013. Сборник статей. Коллектив авторов. - М.: Издательство "Весь Мир", 2014. 384 с.

[43] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement 18.06 2014 г.

С подачи России тема обеспечения МИБ заняла прочное место в повестке дня сессий ГА ООН. 8 декабря 2003 г была учреждена Группа правительственных экспертов (ГПЭ) ООН во исполнение резолюции ГА ООН от 29 ноября 2001 г. A/RES/56/19.[44] Проект доклада по итогам работы Группы был подготовлен в 2004 г., однако был принят не сразу из-за разногласий между её членами по трактовке военно-политических аспектов ИКТ, а также самого предмета рассмотрения ГПЭ: содержание информпотоков или лишь вопросы безопасности информационной инфраструктуры?

На 65-й сессии ГА ООН был принят обновленный российский проект данной резолюции. В резолюции отмечалась результативная работа ГПЭ ООН, действовавшей под российским председательством (А.В.Крутских), и подготовленный ею доклад Генсекретаря ООН, посвященный актуальным исследованиям угроз в области МИБ.

Третья ГПЭ из 15 стран была учреждена резолюцией ГА ООН от 2 декабря 2011 г. (A/RES/66/24), в которой Россию представлял Специальный координатор по вопросам политического использования ИКТ, Посол по особым поручениям МИД России А.В. Крутских. 24 июня 2013 г. доклад ГПЭ был принят консенсусом (A/68/98).[45]

Работа третьей ГПЭ была сфокусирована на вопросах применения международного права в отношении деятельности государств, связанной с использованием ИКТ. Ключевой вывод - международное право применимо в сфере использования ИКТ и самих ИКТ. В докладе отмечена важная роль Устава ООН в поддержании мира и стабильности в информационной среде, подчеркивается принцип государственного суверенитета и вытекающие из него международные нормы и принципы, которые распространяются на деятельность госу-

[44] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf?OpenElement 18.06.2014 г.
[45] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/469/59/PDF/N1046959.pdf?OpenElement 18.06.2014

дарств в сфере ИКТ, а также на юрисдикцию государств над ИКТ-инфраструктурой на их территории.

27 декабря 2013 г. ГА ООН приняла очередную резолюцию (A/RES/68/243) «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[46] (Приложение № 1). Её соавторами наряду с Россией стали 40 стран.

Резолюция призывает государства-члены и далее содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере МИБ, а также возможных стратегий по рассмотрению угроз, возникающих в этой сфере, исходя из необходимости сохранить свободный поток информации.

Имеется в виду, что целям таких стратегий способствовало бы продолжение изучения соответствующих международ-

[46] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/454/05/PDF/N1345405.pdf?OpenElement 18.06.2014

ных концепций, которые были бы направлены на укрепление безопасности глобальных ИТКС.

Принимая во внимание рекомендации, содержащиеся в докладе ГПЭ, резолюция призывает все государства-члены и в дальнейшем продолжать информировать Генсека ООН о своей точке зрения и об оценках по следующим вопросам:

a) общая оценка проблем информационной безопасности;

b) усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области;

c) содержание концепций;

d) возможные меры, которые могли бы быть приняты международным сообществом для укрепления информбезопасности на глобальном уровне.

Отмечено, что ГА ООН просит Генсека с помощью ГПЭ, которая должна быть создана в 2014 г. на основе справедливого географического распределения, а также с учетом рекомендаций, содержащихся в упомянутом выше докладе, и в целях содействия выработке общего понимания продолжить исследование существующих и потенциальных угроз в сфере информбезопасности и возможных совместных мер по их устранению, включая нормы, правила или принципы ответственного поведения государств и меры укрепления доверия, вопросов использования ИКТ в конфликтах и того, как международное право применяется к использованию ИКТ государствами, а также упомянутых выше концепций.

Следует подчеркнуть, что в 2011–2014 гг. усилия российской дипломатии по продвижению МИБ вышли на принципиально новый уровень по следующим трем составляющим:

Первое. Выработка и активное продвижение на международной арене проектов международных документов, регулирующих глобальную политику в сфере использования ИКТ как за счет механизмов мягкого права, так и путем принятия юридически обязывающих конвенций ООН. Ключевая инициатива в этом перечне – концепция Конвенции об обеспече-

нии МИБ[47], презентация которой прошла 1 ноября 2011 г. на первой международной Конференции по вопросам киберпространства в Лондоне.

Концепция Конвенции - это знаковая международно-правовая новация, т.к. она в числе прочего:

• претендует на всеобъемлющий характер и полный охват проблематики МИБ, предлагая принципы и меры для обеспечения комплексного предупреждения и противодействия всей триаде угроз, связанной с использованием ИКТ в области международной безопасности;

• должна через механизм ООН получить глобальный охват и распространить свое действие на все государства-члены ООН;

• предполагает юридически обязывающий характер (не ограничиваясь заявлениями и формулированием общих принципов поведения государств в информационном пространстве);

• позиционируется не как завершенный документ, а как приглашение к доработке и превращению его в действующий международно-правовой инструмент ООН. Текст концепции Конвенции, перспективы его доработки и критические замечания по документу обсуждались 6-8 июня 2012 г. на третьей международной встрече высоких представителей, курирующих вопросы безопасности, в Санкт-Петербурге[48].

12 сентября 2011 г. Генсеку ООН было направлено письмо от Постпредов в ООН четырех государств-членов ШОС - России, Китая, Узбекистана и Таджикистана.[49] К письму прилагался проект «Правил поведения в области обеспечения МИБ», который был распространен в качестве «пищи для

[47] http://www.scrf.gov.ru/documents/6/112.html 18.06.2014
[48] http://www.scrf.gov.ru/news/719.html 18.06.2014
[49] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/58/PDF/N1149658.pdf?OpenElement 19.06.2014

размышлений» на 66-й сессии Генассамблеи ООН.[50] В отличие от концепции Конвенции Правила не носят юридически обязывающего характера, но в целом отражают проблематику концепции Конвенции.

Кроме того, Россия стала одним из инициаторов принятия Решения Постсоветом ОБСЕ от 3 декабря 2013 г. № 1106: «Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью снижения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий» (Приложение № 2).

Второй составляющей усилий российской дипломатии по продвижению МИБ в 2011-2014 гг. стал значительный акцент на двусторонний формат сотрудничества.

3.1.2. МИБ – особенности подхода США и их союзников

Работа ГПЭ продвинула понимание российской позиции по проблематике МИБ. Это выразилось и в трансформации позиции США, которые перестали отрицать важность проблем, связанных с использованием ИКТ государствами в военно-политических целях.

Так, в мае 2011 г. Белым домом США была обнародована «Международная стратегия по действиям в киберпространстве» («International Strategy for Cyberspace»).[51] В ней США впервые приравняли акты компьютерных диверсий к традиционным военным действиям, оставив за собой право реагировать на них всеми средствами вплоть до применения ядерного оружия. Ее логическим развитием в военном измерении стала «Стратегия Министерства обороны по действиям в ки-

[50] http://www.mid.ru/bdomp/ns-dmo.nsf/564e3aa14288230f432569ff003cce37/37afc3dc9bfaebc844257b8f003d66ad!OpenDocument 18.06.2014

[51] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf 19.06.2014

берпространстве» («Department of Defense Strategy for Operating in Cyberspace»), которая была частично рассекречена и опубликована в июле 2011 г.[52] В ней было впервые сформулировано понимание киберпространства как пятой нефизической среды для вооруженных сил США наряду с сушей, морем, воздухом и космосом.

В феврале 2013 г. свою стратегию кибербезопасности принял Евросоюз, которая органично вписалась в контекст Общей политики в области безопасности и обороны ЕС (CSDP) (Joint Communication to the European Parliament, the Council, the European Economic And Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace. Brussels, 7.2.2013 JOIN(2013) 1 final // European Union External Action Website. February 2013.).[53]

В документе отмечается, что наряду с формированием технологического потенциала европейской кибероборонысредстоит сформировать ее доктринальное видение, в т.ч. разделение функций между ЕС и НАТО, между ЕС и странами-членами. Документ содержит проработанный раздел по международному сотрудничеству в сфере кибербезопасности. Одной из ключевых задач ЕС в киберпространстве определено продвижение прав и свобод человека, перечисленных в Хартии ЕС по правам человека.

При этом подчеркивается, что ЕС не требует создания новых международно-правовых инструментов для регулирования вопросов, связанных с киберпространством.

Анализ аналогичных документов союзников США по НАТО, а также большинства стран ЕС показывает, что они имеют схожие подходы к этой проблеме.

[52] http://www.defense.gov/news/d20110714cyber.pdf 19.06.2014
[53] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf 18.06.2014

В этом контексте следует подчеркнуть, что в докладе Генсека ООН от 15 июля 2011 г. (A/66/152)[54] отмечен ответ Правительства США, в котором среди мотивов деятельности, создающей угрозы работе глобальной сети и критических инфраструктур, упоминается перенесение традиционных форм государственного конфликта в киберпространство. В докладе также отмечено, что в ряде обстоятельств подрывная деятельность в киберпространстве может представлять собой вооруженное нападение.

Таким образом, **США видят проблему использования ИКТ для международной безопасности прежде всего в плоскости безопасности информационной инфраструктуры, а не контента трансграничных информационных потоков.**

Наряду с многосторонним форматом в рамках работы ГПЭ, где удалось выработать компромиссную терминологию: изъят западный термин кибербезопасность и практически отсутствовал термин обеспечения МИБ, проводились и двусторонние дискуссии.

3.1.3. Двусторонний формат сотрудничества Россия-США

Работа в двустороннем формате с США была начата еще в 1998 г. Её итогом стало Совместное российско-американское заявление об общих вызовах безопасности на рубеже XXI века, которое 2 сентября 1998 г. подписали в Москве президенты двух стран.[55]

В заявлении признавалась задача ослабления действия негативных аспектов ИКТ для обеспечения стратегических интересов безопасности двух стран, однако документ не

[54] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/416/93/PDF/N1141693.pdf?OpenElement 17.06.2014

[55] https://groups.google.com/forum/#!topic/newsguy.world.gov.diplomatic.security/CEiLS6qOkwA 18.06.2014

предлагал четкой программы международного сотрудничества. Акцент в заявлении был сделан на решении актуальной в тот момент задачи совместного преодоления «проблемы-2000».

Двусторонний формат сотрудничества получил развитие в 2011 г. когда было опубликовано совместное заявление заместителя Секретаря Совбеза России Н.В.Климашина и координатора Белого дома по кибербезопасности Говарда Шмидта.[56] В этом заявлении были названы такие перспективные форматы сотрудничества, как регулярные обмены информацией между национальными центрами реагирования на компьютерные инциденты (CERT), а также оперативный обмен информацией по вопросам кибербезопасности по горячим линиям связи Москва - Вашингтон.

Однако потребовалось два года, чтобы достичь соглашения о мерах доверия в киберпространстве. На полях саммита G8 в Дублине 17 июня 2013 г. пакет из трех соглашений был подписан в ходе встречи В.В.Путина и Барака Обамы. Их подписание сопровождалось совместным заявлением президентов двух стран.[57] (Приложение № 3)

Соглашения предусматривали ряд мер доверия в области использования ИКТ: оперативный обмен данными о киберинцидентах через каналы национальных центров реагирования на компьютерные инциденты (CERT) и центров по уменьшению ядерной опасности (НЦУЯО).

Третьим элементом соглашений стало создание устойчивого контакта между должностными лицами высокого уровня через организацию линии прямой связи по вопросам урегулирования опасных ситуаций в сфере использования ИКТ. Для этого в рамках Президентской комиссии РФ - США создается двусторонняя рабочая группа по вопросам угроз в сфере использования ИКТ и самим ИКТ в контексте международной

[56] http://www.whitehouse.gov/sites/default/files/uploads/2011_klimashin_schmidt_cyber_joint_statement.pdf 19.06.2014
[57] http://news.kremlin.ru/ref_notes/1479/print 19.06.2014

безопасности. С российской стороны эту группу возглавил Н.В.Климашин.

Подписанные соглашения можно было считать прорывом в российско-американском сотрудничестве по вопросам безопасности киберпространства.

Вместе с тем, в связи со «Snowdengate», а также кризисом на Украине последовали санкции США и их союзников. Наиболее отчетливо это проявилось на их ограниченном участии в традиционной конференции по данной проблематике в Гармиш-Партенкирхене в апреле 2014 г.

В Москве такое решение восприняли с недоумением. Только что назначенный Спецпредставитель Президента России по вопросам координации международного сотрудничества в области информационной безопасности, Посол по особым поручениям МИД России А.В. Крутских, участвовавший в работе конференции, заявил следующее: «Противостояние и санкции откинули нас в плане договоренностей в сфере обеспечения международной информационной безопасности на десять лет назад…».[58]

3.2. Нормативно-правовое обеспечение МИБ в России

К третьей составляющей активности России по продвижению МИБ следует отнести значительную работу по совершенствованию национального законодательства.

Ключевыми шагами в этом направлении стали утвержденные Президентом России 12 февраля 2013 г. новая редакция Концепции внешней политики России и 24 июля 2013 г. (Пр-1753) «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года»[59] (далее – Основы). (Приложение № 4, 5)

[58] http://www.kommersant.ru/pda/kommersant.html?id=2459073 19.06.2014
[59] http://www.scrf.gov.ru/documents/6/114.html 19.06.2014

Основы не следует считать прямым ответом «Международной стратегии для киберпространства» США от 2011 г., ибо американская Стратегия наряду с вопросами безопасности охватывает гораздо более широкий круг вопросов с упором на свободу в Интернете, экономическую функцию ИКТ и личную безопасность пользователей.

В России подобные нормы регулируются отдельными нормативно-правовыми актами.

Так, в 2011 г. в Минобороны России были разработаны «Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве».[60] - по сути, прообраз доктрины действий ВС РФ в условиях современной информационной войны. В документе отмечается важная роль информационной работы непосредственно в ходе конфликта с целью эффективнее влиять на его деэскалационное развитие.

Вопросы обеспечения национальной безопасности России в киберпространстве решаются и на институциональном уровне, в том числе в части кибероборонны. Так, в марте 2012 г. вице-премьер Д.О.Рогозин, объявил о возможности создании в России киберкомандования[61].

В связи с вскрытым лабораторией Касперского фактом кибератак на дипломатические и госучреждения России (рис. 3.1.) особое место занимает Указ Президента России от 15 января 2013 г. № 31с[62] (Приложение № 6).

[60] http://function.mil.ru/news_page/country/more.htm?id=10845074@cmsArticle 18.06.2014
[61] http://ria.ru/defense_safety/20120321/601798789.html 18.06.2014
[62] http://www.rg.ru/2013/01/18/komp-ataki-site-dok.html 19.06.2014

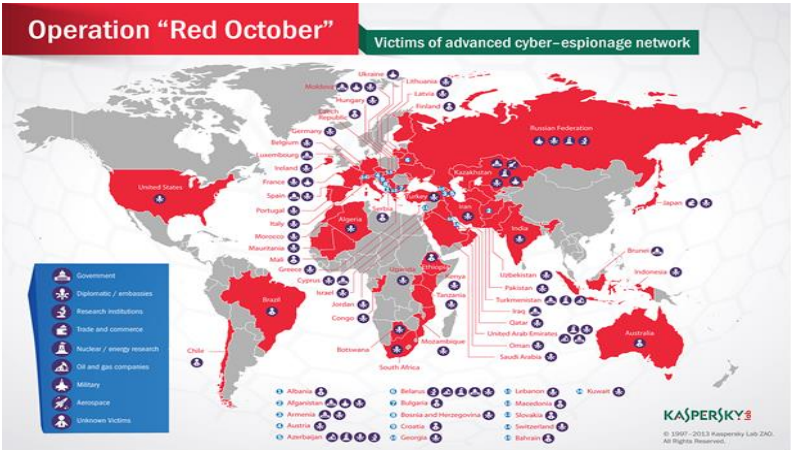


Рис. 3.1.

Указ возложил на ФСБ России создание «государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

3.2.1. Новая редакция Концепции внешней политики России о МИБ

В Концепции внешней политики России впервые введено понятие «мягкой силы» и использование ИКТ. В п.20 второго раздела «Современный мир и внешняя политика Российской Федерации» это изложено следующим образом: «Неотъемлемой составляющей современной международной политики становится «мягкая сила» - комплексный инструментарий решения внешнеполитических задач с опорой на возможности гражданского общества, информационно-коммуникационные, гуманитарные и другие альтернативные классической дипломатии методы и технологии. Вместе с тем усиление глобальной конкуренции и накопление кризисного потенциала ведут к рискам подчас деструктивного и противоправного использования «мягкой силы» и правозащитных

концепций в целях оказания политического давления на суверенные государства, вмешательства в их внутренние дела, дестабилизации там обстановки, манипулирования общественным мнением и сознанием, в том числе в рамках финансирования гуманитарных проектов и проектов, связанных с защитой прав человека, за рубежом.»

В п. 32 раздела III. Приоритеты Российской Федерации в решении глобальных проблем (подраздел «Укрепление международной безопасности») впервые приоритетно обозначена проблема МИБ.

«32. Россия последовательно выступает за снижение роли фактора силы в международных отношениях при одновременном укреплении стратегической и региональной стабильности. В этих целях Российская Федерация:

…з) будет принимать необходимые меры в интересах обеспечения национальной и международной информационной безопасности, предотвращения угроз политической, экономической и общественной проблема безопасности государства, возникающих в информационном пространстве, для борьбы с терроризмом и иными криминальными угрозами в сфере применения информационно-коммуникационных технологий, противодействовать их использованию в военно-политических целях, противоречащих международному праву, включая действия, направленные на вмешательство во внутренние дела, а также представляющие угрозу международному миру, безопасности и стабильности;

и) будет добиваться выработки под эгидой ООН правил поведения в области обеспечения международной информационной безопасности…»

3.2.2. Базовые положения «Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года»

Основами определены основные угрозы в области МИБ, цель, задачи и приоритетные направления госполитики России в данной области, а также механизмы их реализации.

Основы конкретизируют отдельные положения Стратегии национальной безопасности России до 2020 года, Доктрины информационной безопасности России, Концепции внешней политики России и других документов стратегического планирования России.

В Основах под МИБ понимается такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

Основными направлениями госполитики России, связанной с решением задачи по формированию системы МИБ на двустороннем, многостороннем, региональном и глобальном уровнях, являются:

а) создание условий для продвижения на международной арене российской инициативы в необходимости разработки и принятия государствами - членами ООН Конвенции об обеспечении МИБ;

б) содействие закреплению российских инициатив в области формирования системы МИБ в итоговых документах, изданных по результатам работы ГПЭ ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также содействие выработке

под эгидой ООН правил поведения в области обеспечения МИБ, отвечающих национальным интересам России;

в) проведение на регулярной основе двусторонних и многосторонних экспертных консультаций, согласование позиций и планов действий с государствами - членами ШОС, государствами - участниками СНГ, государствами - членами ОДКБ, государствами - участниками БРИКС, странами - членами АТЭС, странами - членами «Группы восьми», «Группы двадцати», другими государствами и международными структурами в области МИБ;

г) продвижение на международной арене российской инициативы в интернационализации управления ИТКС «Интернет» и увеличение в этом контексте роли МСЭ;

д) организационно-штатное укрепление структурных подразделений федеральных органов исполнительной власти, участвующих в реализации госполитики России, а также совершенствование координации деятельности федеральных органов исполнительной власти в данной области;

е) создание механизма участия российского экспертного сообщества в совершенствовании аналитического и научно-методического обеспечения продвижения российских инициатив в области формирования системы МИБ;

ж) создание условий для заключения между Россией и иностранными государствами международных договоров о сотрудничестве в области МИБ;

з) усиление взаимодействия в рамках Соглашения между правительствами государств - членов ШОС о сотрудничестве в области обеспечения МИБ и содействие расширению состава участников указанного Соглашения;

и) использование научного, исследовательского и экспертного потенциала ООН, других международных организаций для продвижения российских инициатив в области формирования системы МИБ.

Общая координация деятельности федеральных органов исполнительной власти, связанной с реализацией

госполитики России, а также с продвижением согласованной позиции России по этому вопросу на международной арене, осуществляется МИД России.

3.2.3. Основные угрозы в области МИБ

Основные угрозы в области МИБ (рис. 3.2.):

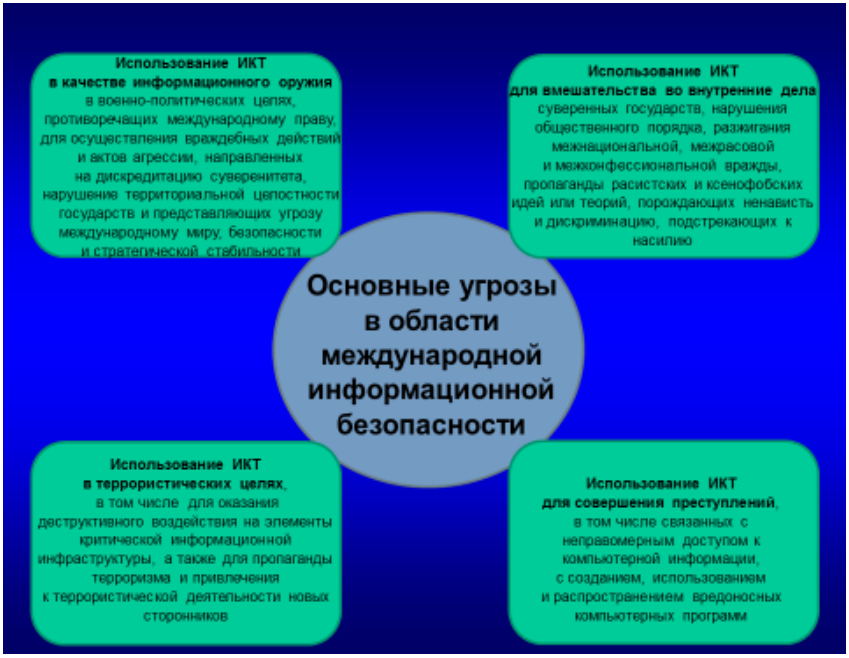


Рис. 3.2.

3.2.3.1. Военно-политическая страта

Военно-политической угрозой в области МИБ Основами определено использование ИКТ в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию су-

веренитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

Основными направлениями госполитики России на данном треке являются:

а) развитие диалога с заинтересованными государствами о национальных подходах к противодействию вызовам и угрозам, возникающим в связи с масштабным использованием ИКТ в военно-политических целях;

б) участие в выработке на двустороннем и многостороннем уровнях мер по укреплению доверия в области противодействия угрозам использования ИКТ для осуществления враждебных действий и актов агрессии;

в) содействие развитию региональных систем и формированию глобальной системы МИБ на основе общепризнанных принципов и норм международного права (уважение государственного суверенитета, невмешательство во внутренние дела других государств, неприменение силы и угрозы силой в международных отношениях, право на индивидуальную и коллективную самооборону, уважение прав и основных свобод человека);

г) содействие подготовке и принятию государствами - членами ООН международных правовых актов, регламентирующих применение принципов и норм международного гуманитарного права в сфере использования ИКТ;

д) создание условий для установления международного правового режима нераспространения информационного оружия.

Рис. 3.3.

Рис. 3.4.[63] (подробно рассмотрено в главе 4)

[63] См. Война в киберпространстве: уроки и выводы для России http://www.belvpo.com/ru/32795.html 19.06.2014

3.2.3.2. «Цифровой джихад»: ИКТ в террористических целях

В Основах угрозой определено использование ИКТ в террористических целях, в т.ч. для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников.

Основными направлениями госполитики России, связанной с решением задачи по формированию механизмов международного сотрудничества в области противодействия угрозам использования ИКТ в террористических целях, являются:

а) развитие сотрудничества с государствами-членами ШОС, государствами-участниками СНГ, государствами-членами ОДКБ, государствами-участниками БРИКС, способствующего предупреждению, выявлению, пресечению, раскрытию и расследованию актов деструктивного воздействия на элементы национальной критической информационной инфраструктуры, минимизации последствий реализации таких актов, а также противодействию использования ИТКС «Интернет» и других ИТКС в целях пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

б) содействие подготовке и принятию государствами-членами ООН, определяющего порядок обмена информацией о передовых практиках в области обеспечения безопасности функционирования элементов критической информационной инфраструктуры.

Ряд экспертов считают, что кибертерроризмом могут быть признаны только действия индивидов, независимых групп или организаций. Любая форма кибератак, предпринимаемая

правительственными и иными государственными организациями является проявлением кибервойны.[64]

По сообщению «Российской газеты» от 12 мая 2014 г. в Вооруженных силах России созданы войска информационных операций.[65] Главное предназначение нового рода войск - защита российских военных систем управления и связи от кибертерроризма и надежное закрытие проходящей в них информации от вероятного противника. В состав информвойск войдут части и подразделения в военных округах и на флотах, укомплектованные высококвалифицированными специалистами: математиками, программистами, инженерами, криптографами, связистами, офицерами радиоэлектронной борьбы, переводчиками и другими.

3.2.3.3. ИКТ и суверенитет России

В Основах угрозой определено использование ИКТ для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию.

Основными направлениями госполитики России, связанной с решением задачи по созданию условий для противодействия угрозам использования ИКТ в экстремистских целях, в т.ч. в целях вмешательства во внутренние дела суверенных государств, являются:

---

[64] См. Gable, Kelly A. "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent" Vanderbilt Journal of Transnational Law, Vol. 43, No. 1 http://cyber.law.harvard.edu/cybersecurity/?title=Cyber-Apocalypse_Now_-_Securing_the_Internet_Against_Cyberterrorism_and_Using_Universal_Jurisdiction_as_a_Deterrent&redirect=no 19.06.2014

[65] http://www.rg.ru/2014/05/12/infvoyska-anons.htm 19.06.2014

а) участие в разработке и реализации межгосударственной системы мер по противодействию указанным угрозам;

б) содействие созданию международного механизма постоянного контроля за недопущением использования ИКТ в экстремистских целях, в т.ч. в целях вмешательства во внутренние дела суверенных государств.

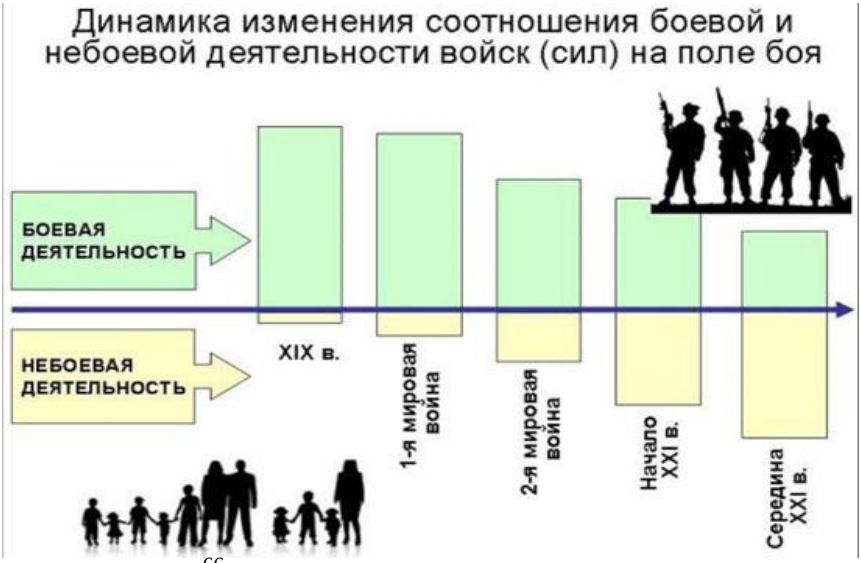


Рис. 3.5.[66] (подробнее рассмотрено в главах 4 и 8)

3.2.3.4. Киберпреступность

Угрозой определено использование ИКТ для совершения преступлений, в т.ч. связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

Основными направлениями госполитики России, связанной с решением задачи по повышению эффективности меж-

[66] См. Подберезкин А.И. Евразийская воздушно-космическая оборона. М.: МГИМО–Университет, 2013. - 488 с. http://www.nasled.ru/?q=print/3274 19.06.2014

дународного сотрудничества в области противодействия преступности в сфере использования ИКТ, являются:

а) продвижение на международной арене российской инициативы в необходимости разработки и принятия под эгидой ООН Конвенции о сотрудничестве в сфере противодействия информационной преступности, а также активизация работы с государствами - членами ШОС, государствами - участниками СНГ, государствами - членами ОДКБ, государствами - участниками БРИКС по поддержке данной инициативы;

б) развитие сотрудничества в сфере противодействия информационной преступности с государствами - членами ШОС, государствами - участниками СНГ, государствами - членами ОДКБ, государствами - участниками БРИКС, странами -членами АТЭС, странами - членами «Группы восьми», «Группы двадцати», другими государствами и международными структурами;

в) повышение эффективности информационного обмена между правоохранительными органами государств в ходе расследования преступлений в сфере использования ИКТ;

г) совершенствование механизма обмена информацией о методиках расследования и судебной практике рассмотрения дел о преступлениях в сфере использования ИКТ.

Рис. 3.6.

Рис. 3.7.[67]

Рис. 3.8.

[67] http://ubr.ua/business-practice/own-business/v-boevoi-gotovnosti-sovremennye-ugrozy-bezopasnosti-kompanii-i-bankov-290010 19.06.2014

3.3. «Таллиннское руководство» по ведению кибервойн НАТО

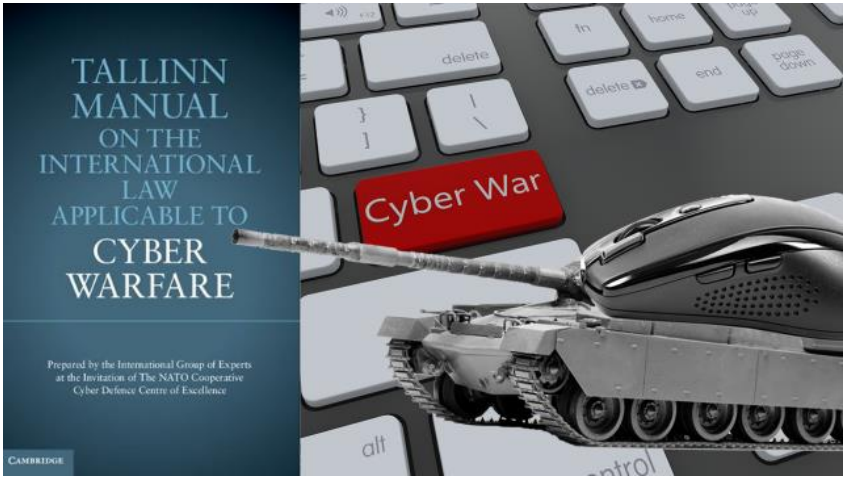


Рис. 3.9.

19 марта 2013 г. Центром совместной киберобороны НАТО в Таллине (CCD COE) был опубликован окончательный вариант Таллинского руководства по вопросам применения международного права к условиям конфликтов в киберпространстве[68]. Речь идет о почти 300-страничном документе, подготовленном группой экспертов Центра в результате трехлетней работы.

Документ привлек к себе внимание прежде всего тем, что ряд его положений при определенных условиях санкционирует применение широкого спектра кинетического оружия против источника киберугрозы, силовые действия военных в отношении гражданских лиц, причастных к кибератакам (за счет причисления их к статусу комбатантов), а также военные кибероперации, направленные против критической инфраструктуры, включая АЭС, дамбы, плотины и т.д.

[68] Michael N. Schmitt. Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2013.

Наличие подобных положений позволило ряду экспертов и дипломатов различных стран утверждать, что Таллиннское руководство дает государствам международно-правовую базу для ведения наступательной кибервойны.

Разработано 95 правил, в т.ч.:

- ответить на атаку государство можно, либо привлекая агрессора к ответственности, либо «пропорциональными контрмерами»;
- считая атаку «вооруженным нападением», правомерна самооборона , в т.ч. и с использованием традиционного оружия;
- кибератаки по силе воздействия следует приравнять к применению химического, биологического и радиологического оружия;
- вооруженным нападением не могут быть признаны кибершпионаж, киберкражи и атаки на сайты (кроме ущерба в государственном масштабе);
- государство-агрессор должно нести ответственность, даже если оно атакует при помощи посредников из других стран.

Таким образом, документ по сути легитимизировал конфликты в киберпространстве как формы поведения государств и действующих в их интересах посредников (proxy actors).[69]

В целом, идея, лежащая в основе документа, представляет собой определенный интерес. Вопрос возникает в отношении особенностей избранного подхода и частично обусловливается международно-политической конъюнктурой, влияющей на интерпретацию выводов и положений документа.

Так, исходя из правил Таллиннского руководства, после атаки боевого кибервируса Stuxnet в 2010 г. на информацион-

[69] «Таллинское руководство» - апология кибервойны?// http://infoshos.ru/ru/?idn=11516 18.06.2014

ные системы центрифуг по обогащению урана Иран был бы правомочен в ответ применить кинетическое оружие.

Некоторый оптимизм в этом смысле внушает доклад третьей ГПЭ ООН, одним из положений которого является консенсус по поводу применимости международного права к информационному пространству.

Именно в «легитимации» конфликтов в киберпространстве российские эксперты видят главный порок Таллинского руководства, в котором отсутствует ключевой посыл о недопустимости кибервойн. При этом руководство активно вплетает правила ведения кибервойн в ткань международного права, да еще и с акцентом на проактивные операции в киберпространстве.

Представляется, что данная проблематика станет предметом активного дискурса в рамках четвертой ГПЭ ООН в 2014 г.

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»

4. СЕТЕЦЕНТРИЗМ: ПАРАДИГМА ГЕОПОЛИТИЧЕСКОГО ДОМИНИРОВАНИЯ XXI ВЕКА

Ведущие западные страны во главе с США, первыми переступив порог информационной эпохи, осуществляют структурную перестройку всех сегментов своего общества, начиная с бизнеса и науки и заканчивая вооруженными силами и системой обеспечения национальной безопасности. Возникают постиндустриальные теории политического устройства, экономики, культуры, коллективной и индивидуальной психологии, военной стратегии, которые, будучи применены в глобальной информационной среде, дают их разработчикам неоспоримые преимущества перед оппонентами, действующими исходя из установок предыдущей фазы исторического развития.

Осуществив переход в постиндустриальную эру, Запад начал вести против России целенаправленные и скоординированные действия, используя новейшие подрывные военно-политические технологии, основанные на гибком применении арсенала информационно-организационного оружия. С распадом СССР внешнее давление не исчезло, а приобрело особо изощренный характер. В повестке дня стоит распад и Российской Федерации (план Бжезинского[70] и др.). Особая ставка

[70] См. З.Бжезинский. Великая шахматная доска. Господство Америки и его геостратегические императивы. - М.: Международные отношения, 2005.

сделана на развал Российской Федерации по «принципу домино», где роль первой костяшки была отведена мятежной Чечне.

4.1. Особенности сетецентрической войны в условиях глобализации

Особенностью современного этапа развития форм, средств и методов подрывной деятельности, проводимой США, является существенное смещение акцентов в ее проведении в сторону реализации «стратегии непрямых действий», целенаправленность, глобальный и системный характер действий по установлению однополярного мира по типу Pax America.

Новые военно-политические сентенции концептуально оформлены в виде стратегии так называемой ***сетецентрической войны***[71] (СЦВ) (Network-Centric War), впервые выдвинутой в 1999 г. сотрудниками RAND Corporation Джоном Аквиллой и Дэвидом Ронфельтом[72], и осуществляются на практике в рамках реализации геополитической концепции окружения Евразии «кольцами анаконды». Дальнейшее развитие концепция ведения СЦВ получила в работе начальника Управления реформирования ВС США (Office of Force Transformation) вице-адмирала Артура Цебровски (Cebrowski)[73] .

Следует отметить, что термин «сетецентризм» впервые появился в компьютерной индустрии и стал результатом про-

---

[71] Следует различать сетецентрическую войну (концентрацию всех имеющихся информационных, политических, военных, экономических и др. ресурсов на поражение (перепрограммирование действий) потенциального противника) от сетевой войны – войны непосредственно в телекоммуникационных сетях посредством боевых кибервирусов, «червей» и т.п., а также проведения информационных операций по дезинформации, уничтожению сайтов и др.

[72] Arquilla J., Ronfeldt D. 1996. *The Advent of Netwar.* Santa Monica.
Ronfeldt D., Arquiila J. 2001. (eds.) *Networks and Netwars.* Santa Monica.

[73] Vice Admiral Cebrowski, Arthur K. and John J. Garstka. Network-Centric Warfare: Its Origin and Future, U.S. Naval Institute Proceedings. Annapolis, Maryland, vol. 124/1/1, January 1998.

рыва в информационных технологиях, которые позволили организовать взаимодействие между множеством компьютеров, даже, несмотря на использование в них разных операционных систем.

В приложении к военному делу *сетецентризм* - более широкое и насыщенное понятие, которое, по сути, определяет парадигму геополитического доминирования XXI века и становится неотъемлемым элементом происходящей революции в военном деле (РВД). Инструментарием достижения новых боевых возможностей, то есть повышения степени реализуемости боевого потенциала, стали современные ИКТ.

Анализ показывает фундаментальную трансформацию в мире от «платформоцентрической» к «сетецентрической войне», которая, по утверждению ее разработчиков, не только определяет новые принципы управления войсками и силами, но и способствует осуществлению РВД на современном этапе. Понятие «сетецентрическая война», или «ведение боевых действий в едином информационно-коммуникационном пространстве», рассматривает боевые формирования как своеобразные устройства (узлы), подключенные к единой распределенной сети. В зависимости от выбора сетевой архитектуры и ее типа такими устройствами могут быть корабли, самолеты, средства поражения, управления, связи, разведки и наблюдения, группа военнослужащих или отдельные солдаты, а также комбинация и тех, и других. В этом случае возможности боевых формирований определяются не столько индивидуальными тактико-техническими характеристиками отдельных образцов ВВТ, сколько возможностями всей группы подключенных к сети средств как единого целого.

Здесь, собственно, и проявляется эффект синергизма, когда целое представляет нечто большее, чем сумма его частей. В приложении к военному делу синергизм – это эффект от совместного действия объединенных в сеть средств вооруженной борьбы, который по совокупному результату превышает сумму эффектов от применения тех же средств по отдельности.

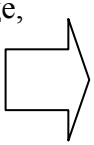
Центральной задачей ведения всех СЦВ является «совокупность действий, направленных на формирование модели поведения друзей, нейтральных сил и врагов в ситуации мира, кризиса и войны». Это означает заведомое установление полного и абсолютного контроля над всеми участниками актуальных или возможных боевых действий и тотальное манипулирование ими во всех ситуациях - и тогда, когда война ведется, и тогда, когда она назревает, и тогда, когда царит мир.[74]

Концепция сетецентрической войны естественным образом включила в себя стратегию непрямых действий, и трансформацию взглядов на ноополитику, и доктрину упреждающих действий (преэмпции) Дж. Буша-мл., а также отражает место и роль технологий информационного противоборства в достижении США глобальной гегемонии во всех сферах мирового пространства и установления окончательного диктата всему мировому сообществу, включая и нынешних союзников по НАТО (рис. 4.1.).

Рис. 4.1. Соотношение составляющих концептов действующих в США доктрин достижения стратегической униполярной гегемонии в XXI веке

[74] Коровин В. Главная военная тайна США. Сетевые войны.- М.: Яуза: Эксмо, 2009.- 288 с.- (Войны XXI века).

где,

 - прямые воздействия «по восходящей» траектории;

 - обратные воздействия «по нисходящей» траектории.

Ключевым понятием для всей теории СЦВ является термин «сеть». В современном «американском» языке помимо существительного «the network» – «сеть» – появился неологизм – глагол «to network», что приблизительно переводится как «охватить сетью», «внедрить сеть в», «подключить к сети». Смысл «сети», «сетевого принципа» состоит в том, что главным элементом всей модели является «обмен информацией» – максимальное расширение форм производства этой информации, доступа к ней, ее распределения, обратной связи. «Сеть» представляет собой новое пространство – информационное пространство, в котором и развертываются основные стратегические операции – как разведывательного и военного характера, так и операции, направленные на «мягкий» перехват власти (управления) в той или иной стране, а также их медийное, дипломатическое, экономическое и техническое обеспечение. «Сеть» в таком широком понимании включает в себя одновременно различные составляющие, которые ранее рассматривались строго раздельно. Боевые единицы, система связи, информационное обеспечение операции, формирование общественного мнения, дипломатические шаги, социальные процессы, разведка и контрразведка, этнопсихология, религиозная и коллективная психология, экономическое обеспечение, академическая наука, технические инновации и т.д. – все это отныне видится как взаимосвязанные элементы единой «сети», между которыми должен осуществляться постоянный информационный обмен.

Смысл военной реформы в рамках «новой теории войны» информационной эпохи состоит в одном: создание мощной и всеобъемлющей сети, которая концептуально заменяет собой ранее существовавшие модели и концепции военной стратегии, интегрирует их в единую систему. Война становится сетевым явлением, а военные действия – разновидностью сетевых процессов. Регулярная армия, все виды разведок, технические открытия и высокие технологии, журналистика и дипломатия, экономические процессы и социальные трансформации, гражданское население и кадровые военные, регулярные части и отдельные слабо оформленные группы, наемники и «частные армии» – все это интегрируется в единую сеть, по которой циркулирует информация. Создание именно такой сети составляет сущность военной реформы ВС США.

Внедрение сети представляет собой лишение стран, народов, армий и правительств мира какой бы то ни было самостоятельности, суверенности и субъектности, превращение их в жестко управляемые, запрограммированные механизмы, что означает прямой планетарный контроль - мировое господство нового типа, когда управлению подлежат не отдельные субъекты, а их содержание, их мотивации, действия, намерения и т.д. И враги, и занимающие нейтральную позицию силы, по сути, заведомо подчиняются навязанному сценарию, действуют не по своей воле в соответствии с управляемым процессом рефлексии. Это выигрыш битвы до ее начала.

Цель СЦВ - абсолютный контроль над всеми участниками исторического процесса в мировом масштабе. И здесь необязательны прямая оккупация, массовый ввод войск или захват территорий. Излишни армейские действия и огромные траты на Вооруженные Силы. **Сеть** - более гибкое оружие, она манипулирует насилием и военной силой только в крайних случаях, и основные результаты достигаются влиянием на широкую совокупность факторов - информационных, экономических, социальных и т.д.

4.2. Сетецентризм в действии

Сегодня очевидно **расширение понятия СЦВ до масштабов глобальной информационной агрессии.** Тем более, что новый взгляд на угрозы XXI столетия заключается как раз в том, что все чаще основная угроза исходит не от регулярных армий разных стран, а от всевозможных террористических, криминальных и других организаций, участники которых объединены в некие сетевые структуры.

В сущности, эти сетевые организации переводят информационное превосходство во всю ту же боевую мощь, эффективно связывая интеллектуальные объекты в единое информационное пространство действий. Происходит ***трансформация понятия поля боя в боевое пространство***.[75] В него включены цели, лежащие в виртуальной сфере: эмоции, восприятие и психика ситуативного «противника». Воздействие на новые классы целей достигается за счет тесной интеграции сетевых структур координирующего органа в лице Минобороны США, а также спецслужб и сетевых структур гражданского общества (например, негосударственных общественных объединений, отвечающих за выработку «общественного мнения»).

Между тем, современное противостояние в информационной сфере ведется не только между государствами, но и между негосударственными (неправительственными) организациями (НПО) и государством. Роль НПО в организации и проведении т.н. «цветных революций» хорошо известна[76].

Для достижения своих далеко идущих геополитических целей США прибегают к новейшим технологиям перехвата управления в странах-мишенях, создавая в них управляемые

---

[75] Сетецентризм: геополитические и военно-политические аспекты современности / Под общ.ред. проф. Анненкова В.И. Учебник – М.: РУСАВИА. 2013. с. 21

[76] А.Бовдунов. НПО: сетевая война против России.// Сетевые войны. Угроза нового поколения.- М.: Евразийское движение, 2009.

А.Дугин. Зачем России НПО? Опубликовано в еженедельнике «Южный Федеральный», № 3 (226) от 1-7 февраля 2006.

ими подконтрольные многомерные и современные многосвязные политические, экономические и социальные негосударственные сетевые структуры, которые приводятся в движение по отношению к стране-жертве в критический момент, независимо от существующих в данной стране де-юре формальных политических институтов, электоральных показателей и общепринятых легитимных процедур передачи власти. Если мягкий сценарий легитимной передачи власти не проходит, они добиваются своего иными способами – сетевыми возмущениями, комбинирующими информационные факторы, культурные и психологические коды. Для этого используются гуманитарные фонды, ассиметричные альянсы различных НПО и неформальных объединений, инспирируется мобилизация радикальных групп молодежи и т.д. (рис. 4.2.).

Несмотря на ряд нерешенных проблем и отсутствие даже среди военных специалистов США единого мнения относительно концепции «Сетецентрическая война», обеспечение всесторонней интеграции, повышение уровня взаимодействия, а также достижение синергетического эффекта за счет реализации новых принципов управления и ведения боевых действий становятся неотъемлемым условием реформирования вооруженных сил большинства стран мира.

Но все они, так или иначе, в основе своей содержат принципы именно американского подхода к СЦВ. И поэтому, главное - понять суть американской концепции «Сетецентрическая война», которую один из ее основоположников охарактеризовал следующим образом: «сетецентрическая война для войны, то же самое, что электронный бизнес для бизнеса»[77], или электронное правительство для повышения эффективности деятельности государства в целом.

[77] http://vpk-news.ru/articles/5822

Рис. 4.2. Сетевая организация
неправительственных организаций,
работающих против России.

В итоге происходит пересмотр самого мировоззрения на роль информации и формирование новой культуры информационного обмена. В конечном итоге такой пересмотр приводит к формированию принципиально новых подходов для достижения геостратегических целей за счет монопольного использования информационной сферы в своих интересах.

Стремительное развитие ИКТ, а также опыт применения «оргоружия» накопленный США, как при проведении «цветных революций», так и в ходе «арабской весны», а также госпереворота на Украине в 2014 г., позволил США сделать еще один шаг в развитии методологической базы «четвертой» мировой войны. Этим шагом стало появление новой концепции ведения информационной войны, в которой информационный компонент рассматривается, как доминирующий (при этом силовой компонент не исключается).

Новая концепция позволяет в рамках единого подхода охватить все три уровня информационно-силового противоборства: *стратегический* - уровень, охватываемый понятием «стратегическая информационная война», *оперативный* и *тактический* - уровни, охватываемые понятием «мятежевойна».

4.3. «Мятежевойна» как элемент стратегии ведения СЦВ

Эпоху «мятежевойны» (в ряде трактовок этот термин звучит как «мятежвойна»), наступление которой предсказал еще в начале 60-х гг. XX в. русский военный ученый-эмигрант Евгений Месснер[78], открыли террористические акты в США 11 сентября 2001 г. Месснером были определены принципиальные особенности этого явления: отсутствие линий фронта и четких границ между противниками, превращение общественного сознания в основной объект воздействия, пространство войны становится четырехмерным (к трем традиционным добавляется информационно-психологическое измерение).

Однако Месснер не раскрыл сути методов борьбы с противником, избравшим стратегию «мятежевойны». Первыми попытку восполнить этот вакуум предприняли политики и военные США[79].

Важнейший вывод из сетецентрической концепции для обеспечения военной безопасности и США, и их союзников по НАТО состоит в признании того, что в обозримом будущем ос-

---

[78] Месснер Е.Э. Всемирная мятежевойна. – Жуковский: М.: Кучково поле, 2004.

[79] Network-Centric Warfare: Department of Defense Report to Congress, 27 July 2001.
Шеремет И. Компьютеризация как путь к победе в вооруженной борьбе // НВО № 42 (451). 2005.
Попов И. Сетецентрическая война Пентагона / НВО № 9(369). 2004.
Горбачев Ю.Е. Сетецентрическая война: миф или реальность? // Военная Мысль. 2006. № 1.
Дугин А. Мир охвачен сетевыми войнами // НВО № 44(453). 2005.

новные угрозы их национальным интересам будут исходить не от регулярных армий, а от террористических, криминальных, экстремистских и других преступных сообществ, способных объединяться в региональные или глобальные транснациональные сетевые структуры.

Понимая, что с сетецентрическими структурами можно бороться только с помощью других сетецентрических структур, военно-политическое руководство США отдает предпочтение *невоенным операциям* (Operation Other Then War), что требует организации тесного сетевого взаимодействия между подразделениями ВС с гражданскими государственными и негосударственными организациями, осуществляющими наступательные и оборонительные акции в сфере организационного и информационного противоборства.

Особенность оргоружия, основанного на сетецентрическом принципе, состоит в том, что такие сетевые структуры могут возникать спонтанно, носить временный характер, не иметь четкой иерархической подчиненности, а, зачастую, и единого руководства. Главным объединительным мотивом такой сетевой организации являются мнения, установки и убеждения ее членов и источники финансирования. Объединяясь в небольшие группы, через горизонтальные связи, поддерживаемые с другими сетевыми структурами, они могут превращаться на короткий срок в локальные, региональные и даже в глобальные сетевые структуры, а после достижения своих целей, опять становиться локальной сетевой группой или полностью прекращать свое существование. Выявить и уничтожить такую сетевую структуру достаточно сложно, поскольку она, как правило, не имеет четко очерченных географических и исторических границ, однозначного центра, а значит выраженной устойчивой иерархии, уничтожением которой можно было бы разрушить всю систему. Более того, если даже центральный орган, будет все-таки локализован или уничтожен, лидерство в сети автоматически переходит к другому центру.

Взаимодействия членов сообщества в такой сетевой структуре, как правило, организованы по принципу «стаи». В повседневной жизни отношения членов сетевого сообщества носят спонтанный, чисто символический характер. В определенный момент времени члены сетевого сообщества, мотивированные общей целью на то или иное совместное действие, по сигналу-наводке, исходящему от любого из ее членов, собираются в условленном месте в «стаю», участвуют в теракте, нападении, бандитской вылазке. Сразу после ее завершения «стая» прекращает свое существование. Ее члены вновь превращаются в законопослушных, мирных граждан. Подвергнутая нападению «стаи» сторона часто не может идентифицировать, кем, откуда и с какой целью была проведена такого рода акция, а потому не способна нанести ответный удар, чтобы наказать виновных и, тем самым, не допустить повторения аналогичных действий в будущем. Именно в этом заключается высокая живучесть и целевая эффективность оргоружия, организованного по сетецентрическому принципу.

Сетецентрические войны по принципу «стаи» могут вестись не только криминальными, террористическими и экстремистскими организациями, но и легитимными, в том числе финансовыми и другими неправительственными национальными и транснациональными организациями (например, захват чужого имущества с помощью механизма рейдерства). Для успешного проведения таких «активных» специальных акций на временной или постоянной основе в состав членов сетевой структуры включаются их представители, внедренные в правительство, в законодательные и правоохранительные органы, которые располагают необходимой оперативной информацией и обеспечивают оперативное прикрытие в случае непредвиденных обстоятельств. Благодаря этому, государство превращается в политический инструмент, который отдельные легитимные и теневые сетевые структуры используют для достижения своих целей, в ущерб национальным интересам. По этой причине процесс глобализации, инициатором ко-

торого выступают США и страны «золотого миллиарда», - процесс формирования и постоянного реконфигурирования глобальных транснациональных горизонтальных сетевых из локальных национальных организационных сетевых структур, игнорирующих национальный суверенитет государств и национальную самобытность народов, которые в этот миллиард не попали. За множеством таких сетевых структур, в том числе и сетей, элементами которых являются отдельные государства, стоят надгосударственные международные сетевые структуры — *инициаторы* процесса глобализации, государственные и негосударственные сетевые структуры - проектировщики и генеральные директоры, управляющие глобальными сетевыми ресурсами, а также сетевые структуры - доноры, которые несут всю тяжесть последствий глобализации. При этом в различные моменты истории одни и те же сетевые структуры могут занимать различное положение в общей иерархии, выстраиваемой инициаторами процесса глобализации: из разработчиков и сетевых менеджеров могут превращаться в исполнителей, распорядителей и даже сетевых доноров.

Международные сетевые структуры - инициаторы процесса глобализации, которые принято называть «мировой закулисой», представлены закрытой для посторонних сетью чрезвычайно влиятельных *неправительственных организаций* (НПО). Их сетевая структура также не имеет четкой иерархии, географической привязки, устава, постоянного членства, функционирует по принципу «стаи». Эти сетевые структуры способны через своих представителей в сетевых структурах более низкого международного статуса оказывать серьезное влияние на всю мировую политику, финансовую систему, экономику, принимать и проводить решения о смене политических режимов, изменению курса развития той или иной страны и др.

За счет мобилизации сетевых ресурсов, находящихся под контролем этих представителей, мировое сообщество может в «мягкой» форме направляться на решение, широкого круга четко фиксируемых и координируемых задач в сфере внутрен-

ней и внешней политики. Благодаря формированию такой пространственно разнесенной и иерархически упорядоченной мета-сетевой организации, верхние этажи которой занимают сети, принадлежащие западному сверхобществу, реализуется фарисейский по своей сути принцип управления миром, когда управляемый субъект либо не понимает, что им управляют, а если и понимает, то не может определить, из какого центра происходит это управление, и кто несет за него ответственность.

По этой причине главной *задачей,* решаемой в ходе ведения глобальных и региональных информационных войн, является создание глобального по масштабам, не имеющего разрывов мета-сетевой структуры единого информационного пространства человечества, способной обеспечить в обозримом будущем тотальную *наблюдаемость* и *управляемость* над процессами, происходящими в любой точке мирового пространства. По существу эта глобальная, многоуровневая мета-сетевая информационно-психологическая структура человечества представляет собой кибернетический аналог «ноосферы»[80] (рис. 4.3.).

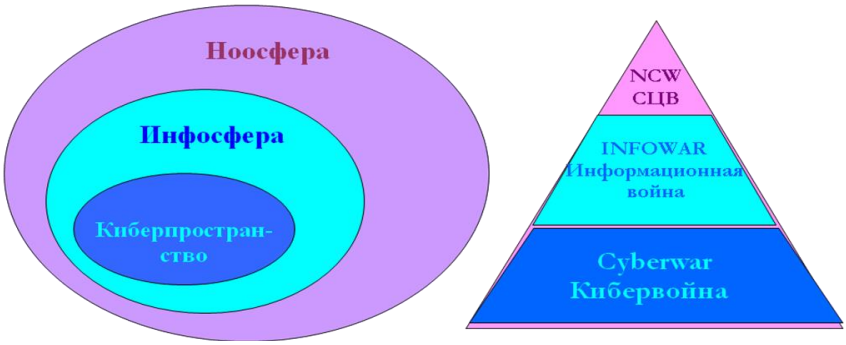


Рис. 4.3. Три области обращения информации - три сферы информационных конфликтов

[80] Термин был введен французскими учеными П.Тейяр-де-Шарденом и Ле Руа после цикла лекций в Сорбонне В.И.Вернадским. В конце своей жизни Вернадский согласился с термином и развил ряд его составляющих.

В этом всеобъемлющем сетевом кибер-«ноосферном» пространстве любая глобальная или локальная сетевая структура должна служить не только источником объективной информации обо всех происходящих в зоне их экономической, политической и идеологической ответственности для сетевых структур более высокого уровня иерархии, но и без особых усилий должна трансформироваться в сетевое оргоружие, направляемое против любой проявляющей свою самостоятельность или непокорность вертикальной сетевой оргструктуры (государства), с целью показательной для других сетевых структур «нормализации» ее поведения.

Можно утверждать, что за достижение именно этой глобальной мета-сетевой информационной и транспортно-коммуникационной «прозрачности» велась вооруженная борьба в бывшей Югославии, Афганистане, Ираке, Ближнем Востоке, именно для этого осуществлялись и будут осуществляться цветные, бархатные революции на постсоветском пространстве.

4.4. Стратегия непрямых действий и «цветные революции»

Модели невооруженного перехвата власти в рамках реализации «***стратегии непрямых действий***» (СНД) апробируются при проведении так называемых «цветных революций»[81]. Новейшие стратегии бесконтактных войн шестого поколения активно внедряются в практику ведения боевых действий США в Ираке и Афганистане, тестируются и верифицируются в ходе различных учений и на специализированных симуляторах. Разработчики теории СЦВ, построенной на сетевых принципах ведения войны в информационную эпоху,

[81] Глазунов О.Н. Государственный переворот. Стратегии и технологии. – М.: ОЛМА-ПРЕСС Образование, 2006. – с.448 (Досье). Раскин А.В., Пеляк В.С. К вопросу о сетевой войне // Военная Мысль. 2005. № 3

убеждены, что она существенно и необратимо изменила традиционную технологию ведения наступательных войн, о чем не раз в своих докладах упоминали руководители Пентагона.

В новых исторических условиях под СНД следует понимать искусство комплексного воздействия, направленного на дестабилизацию общества изнутри. СНД позволяет реализовывать крупные геополитические проекты, например, перераспределение сфер влияния, раскол государств и союзов, предотвращение образования новых союзов, создание «буферных зон» и «поясов нестабильности», получение доступа к источникам сырья, рынкам сбыта и т.п. Пример использования сетецентрических операций (СЦО) в рамках СНД приведен на рис. 4.4.

Рис. 4.4. Многомерное пространство
ведения сетецентрических операций

Основу информационно-коммуникационного пространства войны будущего составляет GIG (Global Information Grid) министерства обороны США - так называемая «Глобальная информационная решетка» (ГИР), представляющая собой мощную группировку взаимосвязанных разведывательных, коммуникационных и навигационных космических летательных аппаратов США на околоземной орбите. Именно ГИР связывает оперативным и административным управлением воедино все силы и средства вооруженных сил США и их союзников по НАТО и обеспечивает их всей информацией, необходимой для ведения войны. Она оптимизирует процессы сбора, обработки, хранения, распределения информации и управления ею, а также доведения ее до потребителей внутри министерства обороны и за его пределами. Быстрое развитие компьютерных технологий требует создания новой концепции сетецентрических войн на базе современной интерактивной сети. В плане реализации такой концепции, следующим шагом в достижении решающего информационного превосходства американским стратегам представляется слияние технологий ГИР, Web 2.0 и облачных вычислений.

В связи с формирующимся глобальным информационным обществом, а также появлением новых стратегий враждебных действий против России и в целом на постсоветском пространстве, а именно СНД и СЦВ, необходимо изменить и подходы к моделированию конфликтов, характерных для противоборства в новых условиях сетевизации государственных и социальных институтов.

Проблемы принятия решений в условиях конфликта в информационную эпоху заключаются в генерации альтернатив решений их оценки и выборе оптимальной на основе задан-

ных критериев альтернативы[82]. Предлагается использовать методы эволюционного поиска, гомеостатические и синергетические принципы управления этим поиском для получения оптимального решения[83].

Основные задачи, возникающие при этом, - это обработка знаний, обучение и самообучение, самоорганизация, адаптация к динамично меняющейся среде противоборства, построение из социального хаоса упорядоченных устойчивых социально-экономических систем, реализация экстремальных принципов комплексных воздействий сложной природы, накапливание и обработка разнородной информации, естественное общение с человеком в процессе принятия решения, внедрения принципов рефлексивного управления.

Предложенный В.А.Лефевром метод оценок интенций эксперта (ЛПР) в виде рефлексивных структур и его дальнейшее развитие, основанное на использовании понятий теории нечетких множеств, позволяют проводить количественное рассмотрение динамических автологических систем с элементами психологии[84]. Важнейший для

---

[82] Гаврилов В.М. Оптимальные процессы в конфликтных ситуациях. - М.: Сов. радио,1969.
Крапивин В.Ф. Теоретико-игровые методы синтеза сложных систем в конфликтных ситуациях. - М.: Сов.радио, 1972.
Робинсон Дж. Итеративный метод решения игр. //Сб. «Матричные игры». - М.:Физматгиз, 1961.-с.110-118.
Саати Т.Л. Математические модели конфликтных ситуаций. /Пер. с англ.-М.: Сов. радио, 1977.

[83] Стратонович Р.Л., Гришанин Б.А. Игровые задачи с ограничениями информационного типа.// «Известия АН СССР», Техническая кибернетика, 1968, № 1.
Трахтенгерц Э.А. Компьютерная поддержка принятия решений. М.: Синтег, 1998.
Берштейн Л.С., Карелин В.П., Целых А.Н. Модели и методы принятия решений в интегрированных ИС. Ростов-на-Дону. Изд-во РГУ, 1999.
Горский Ю.М. Основы гомеостатики (Гармония и дисгармония живых, природных, социальных и искусственных систем). Иркутск: Изд-во ИГЭА, 1988.
Хакен Г. Синергетика. Иерархия неустойчивостей в самоорганизующихся системах и устройствах. М.: Мир, 1985.

[84] Лефевр В.А. Конфликтующие структуры. – М.: «Сов. радио», 1973.
Лефевр В.А. Элементы логики рефлексивных игр. Проблемы инженерной психологии. – М.: изд. АН СССР, 1966.

теоретических построений постулат, выдвинутый им, заключается в необходимости учета при планировании информационных операций не только моделей мира, созданных противниками, но и моделей моделей. Использование метода описания процесса осознания мира рефлексивными системами наряду с целостным синергетическим подходом к описанию сетевых конфликтов в условиях сецентрических войн современности дает методологический ключ к моделированию конфликтов в глобальном информационном обществе.

С указанными задачами тесно связаны новые интенсивно развивающиеся науки гомеостатика и синергетика. Гомеостатика - это наука, позволяющая моделировать условия, необходимые для устойчивого функционирования систем, содержащих неустойчивые компоненты. С помощью принципов гомеостатики можно разрабатывать информационные механизмы управления поиском решений. Другими словами, гомеостатика определяет сущность механизмов поддержания равновесия в объектах сложной природы.[85]

Считается, что синергетика - это попытка разработать рациональную модель нерационально устроенного мира.[86] Синергетика, гомеостатика и эволюционное моделирование приближают нас к целостной модели природы и механизмов противоборства в информационную эпоху, состоящую из хаоса и порядка, организации, самоорганизации и дезорганизации, случайности и необходимости, гармонии и дисгармонии, динамизма и гомеостата, сетевых принципов организации и управления.

[85] Горский Ю.М. *Основы гомеостатики* (Гармония и дисгармония живых, природных, социальных и искусственных систем). Иркутск: Изд-во ИГЭА, 1988.
[86] Хакен Г. *Синергетика*. Иерархия неустойчивостей в самоорганизующихся системах и устройствах. М.: Мир, 1985.

4.5. Ситуационный анализ при проведении сетецентрических войн

Сетецентрические войны существенно и необратимо изменили традиционные технологии ведения наступательных войн. Ключевым фактором, движущей силой процесса планирования всех современных сетевых операций в конфликтах нового поколения является анализ ситуации – внешних и внутренних условий обстановки. На нем основаны процедура мониторинга и прогнозирования важнейших элементов базовой модели информационной войны, методология принятия решений, механизм управления на различных этапах стратегического сдерживания. В результате обеспечивается формирование и актуализация исходных данных и знаний, необходимых для проведения сетевых войн.

Ситуационный анализ, в свою очередь, основывается на рефлексивном подходе, который позволяет не только просчитать ходы в вооруженной борьбе, но и запрограммировать исход сетевых операций из особенностей ситуации и личных качеств противника.[87]

Таким образом, ситуационный анализ направлен на уменьшение неопределенности контролируемых и неконтролируемых факторов. На его основе формируется механизм управления современных сетевых операций Запада против России, в т.ч. процедуры принятия решения, планирования боевых или «непрямых» действий, распределения сил и средств, разведывательно-информационного обеспечения и т.д. Однако только качественный анализ, имеющий логико-психологический рефлексивный компонент, предполагает выявить настоящую природу и оценку действий субъектов сетевых войн, найти «скрытые пружины» конфликтной ситуации.

[87] Рефлексия и ее математическое моделирование. Новиков Д.А., Чхартишвили А.Г., 2004

Прогноз последствий рефлексивного управления и оценка вероятности событий основаны на использовании статистических данных, математическом и имитационном моделировании как внешних причин, так и человеческого фактора. Оценка вероятности события на использовании одной лишь статистики, например, о частоте повторения событий (в т.ч. за определенный промежуток времени), существенно затруднена из-за отсутствия необходимых объемов информации. Более точные оценки могут дать имитационные модели, содержащие множество параметров и переменных. Однако они малопригодны для исследования общих закономерностей широкомасштабных явлений, в частности войн и вооруженных конфликтов, терроризма на основе концепции «мятежвойны», социальных потрясений и цветных революций.

4.6. Синергетический подход к описанию сетевых конфликтов

В рамках ведения современных сетецентрических войн и операций особое внимание уделяется реализации синергетических принципов[88]. Выделяются ключевые принципы сетевых конфликтов, анализируются различия в иерархической и сетевой системах управления сложными сетями, важные с точки зрения обеспечения безопасности в контексте возможных воздействий.

Как было отмечено выше, одним из основных принципов проведения сетецентрических операций является достижение информационного превосходства.

---

[88] Glenn E. «*Chaos Theory: The Essentials for Military Applications»* Department of Advanced Research Paper, Naval War College Paper 10, Newport, RI, 21 February 1995. Gregory M. Maguire. CONCEPT OF A DYNAMIC ORGANIZATIONAL SCHEMA FOR A NETWORK-CENTRIC ORGANIZATION. United States Navy B.A., University of Southern California, NAVAL POSTGRADUATE SCHOOL, June 2003. Григорьев В.Р. Сетецентрическая парадигма информационного противоборства с позиции теории управляемого хаоса. Вестник ИКСИ, Серия «В», № 7, инв. 19636, Москва 2010, с. 291-321.

Проведем сравнение моделей достижения информационного превосходства в условиях «классического» и сетецентрического противоборства (рис. 4.5.).

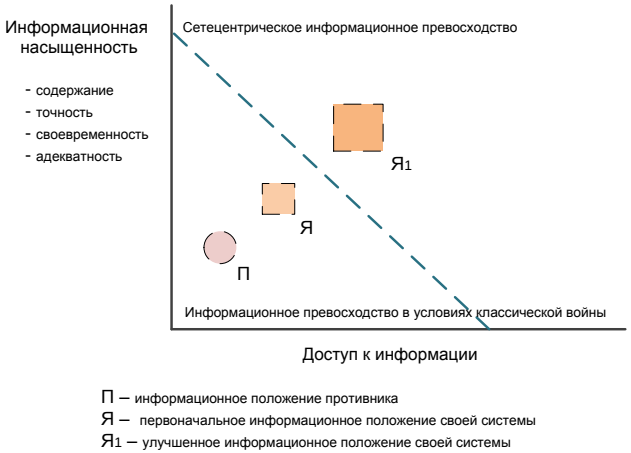


Рис. 4.5. Достижение информационного превосходства в условиях сетецентрического противоборства

Под ***доступом к информации*** подразумевается набор пространственно-временных характеристик, описывающих доступность информации для противоборствующих сторон (о противнике, своих силах, окружающей обстановке и т.д.). ***Информационная насыщенность*** есть интегральная характеристика качества информации (содержание, точность, своевременность, адекватность и т.д.). Эти два аспекта определяют фактическую информационную среду, в которой осуществляются операции. Пунктирной линией обозначен условный предел информационного превосходства в условиях классических и сетецентрических операций. Этот предел обусловлен различиями в уровнях доступа к информации у различных (возможно, смежных) структур сети.

Заметим, что в условиях сетецентрических операций необходимо говорить о единстве следующих сфер: информа-

ционной, физической и когнитивной (познавательной, рационально-ментальной) (рис. 4.6.).

Любые активные операции, в том числе сетецентрические, характеризуются определенной степенью ***динамического хаоса***[89]. На сегодняшний день исход операций во многом зависит от того, насколько та или иная сторона может использовать хаос в своих интересах.

Рис. 4.6.

В этом смысле одним из важнейших с точки зрения практики вопросов является определение границы между хаосом и порядком в реальных сложных системах (рис. 4.7.).

[89] ***Динамический хаос*** – это явление, при котором поведение нелинейной системы выглядит случайным, несмотря на то, что оно определяется детерминистическими законами. Причиной появления хаоса является неустойчивость по отношению к начальным условиям и параметрам: малое изменение начального условия со временем приводит к сколь угодно большим изменениям динамики системы.

Рис. 4.7. Область хаоса и ее пограничная линия

В условиях сетецентрических операций пограничная линия хаоса определяется, в первую очередь, масштабом и интенсивностью осуществляемых воздействий. Чем выше эти показатели, тем труднее контролировать развитие ситуации и, соответственно, тем выше степень хаоса.

На определенном этапе операции может наступить такое состояние, когда становится практически невозможно управлять ходом ее развития. Иначе говоря, система попадает в область хаоса. В области порядка лежат операции, которые можно организованно планировать и осуществлять на практике.

Операции, проводимые в области хаоса, являются столь масштабными и быстротечными, что эффективно контролировать их – чрезвычайно сложная задача. В этом смысле на первый план выходит вопрос подготовки выгодных начальных условий для целевой системы, из которых она с определенной (достаточной) вероятностью может перейти в желаемое состояние.

Следует отметить, что сама граница хаоса не представляет собой четко фиксированную линию. Она может изменять свои параметры в соответствии с уровнем подготовки операции. Чем тщательнее спланирован ход событий, чем лучше

учтены необходимые факторы, тем шире будет зона порядка. С точки зрения возможных активных воздействий на вероятного противника ситуация обратная: чем более полно использованы характерные особенности его сетевой структуры при планировании операции, тем вероятнее траектория функционирования его системы попадет за границу хаоса, которая в этом случае будет ближе.

Если наложить графики, описывающие границы областей хаоса для своей системы и системы противника, то вместо двух областей – порядка и хаоса – появятся три области: полный порядок, полный хаос и промежуточная зона – ***сфера асимметричности***. В этой зоне более подготовленная сторона будет действовать в рамках порядка, а менее подготовленная – в рамках хаоса (рис. 4.8.).

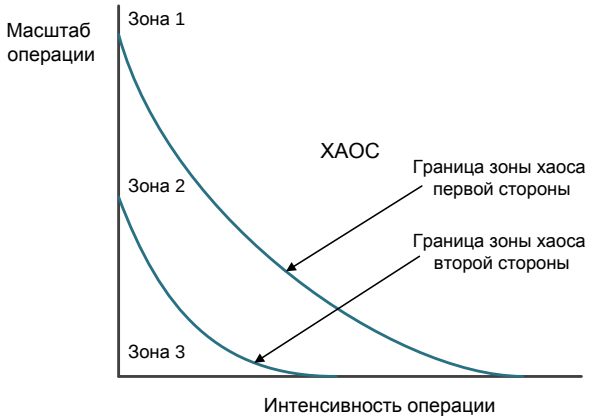


Рис. 4.8. Операции на границе зон хаоса

Операции, проводимые в сфере асимметричности (зона 2) характерны для ***симметричных конфликтов***, в которых противоборствующие стороны ведут свои действия «по правилам», используя свои основные (регулярные) силы. Исход таких конфликтов во многом определяется способностями сторон максимально «отодвинуть» свою границу зоны хаоса,

чтобы воспользоваться преимуществами над противником, которому навязываются действия в его сфере хаоса.

Ситуация меняется в случае ***асимметричного конфликта*** (рис. 4.9.).

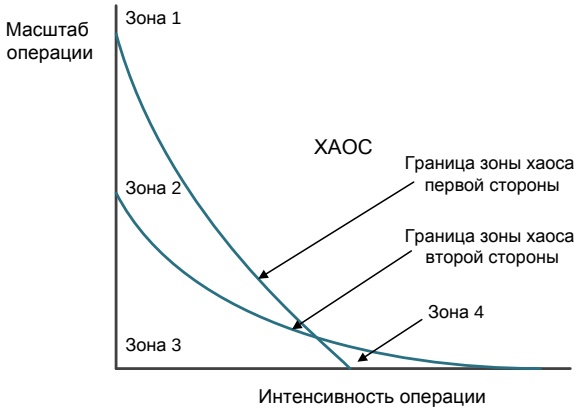


Рис. 4.9. Пересекающиеся границы зон хаоса в ассиметричном конфликте

Помимо зоны 2, в которой одна из сторон имеет преимущество, появляется зона 4, где ситуация меняется на противоположную. Именно наличие этой зоны объясняет, почему не всегда побеждает более сильная во всех отношениях сторона. Бывают ситуации, когда «слабый» противник может прибегнуть к нестандартному для него, асимметричному ответу (например, резко сменит тактику, перейдя от иерархической схемы управления к сетецентрической).

В качестве примера подобных ситуаций можно привести деятельность террористических групп. В ходе проведения ограниченных по масштабам и целям операций пограничные линии зон хаоса противоборствующих сторон могут пересекаться, создавая несколько неустойчивых зон.

Ассиметричный подход террористов обычно состоит в том, что они формируют мелкие отряды, такие, что бороться с ними регулярным войскам и спецслужбам в рамках сло-

жившейся организационно-штатной структуры практически невозможно. Операциями служат многочисленные быстрые рейды, на которые противоборствующая сторона не успевает адекватно реагировать. При этом физический ущерб, наносимый такими «пчелиными укусами», может быть существенно меньше, чем последующий (психологический) эффект от самих фактов их осуществления.

Ассиметричный подход действий экстремистов (мятежников) при проведении «цветных революций» заключается в создании многочисленных очагов массового протеста, привлечения СМИ для создания образа «народного негодования» действующими режимами и доведения его до «демократической общественности», стремлении перетянуть на свою сторону правоохранительные органы.

Радикальное изменение общества - как в сторону перехода к более высокому типу социальной организации, так и в направлении его деградации и распада - осуществляется через прохождение стадии бифуркации. Эта стадия (особенно ее высший пункт - точка бифуркации) характеризуется дезинтеграцией системы, резким ослаблением социального порядка, бурным нарастанием явлений хаоса и распада. Бифуркирующая система находится в состоянии крайней неустойчивости. Происходит борьба различных сил и тенденций, ни одна из которых не является доминирующей. Хаотические, в разных направлениях действия людей и социальных институтов приводят к резкому падению функциональной способности системы. Общество находится в состоянии шаткого равновесия. В этот момент даже случайность, малые флуктуации, незначительные воздействия в период обычного, «нормального» развития общества могут оказать решающее влияние на выбор модели общественного устройства, последующую траекторию исторического развития. **История показывает, что бифуркация в радикальном варианте, как правило, начинается при условии глубокого разложения правящего**

класса, который оказывается критически слабым звеном в структуре системного кризиса.

Победа в асимметричном конфликте напрямую зависит от того, насколько успешно блокируются возможности для перехода противника в зону 4. В этой связи становится наиболее актуальной задача обеспечения готовности своей сети к проведению быстрых точечных операций, направленных на сеть противника. Преимущество в скорости и эффективности управления может быть достигнуто с помощью получения информационного превосходства с позиций сетецентрического подхода.

Информационное превосходство над противником, работающим на уровне террористических или экстремистских групп, дает решающее преимущество над ним. Мелкие группы могут быть нейтрализованы только небольшими, самосинхро-низирующимися, децентрализованными, автономными подразделениями-ячейками, объединенными в единую сеть. Другими словами, необходимо максимально дальше отодвигать границу сферы хаоса, как по оси масштаба операции, так и по оси интенсивности.

Именно этот механизм обеспечивает возможность быстрой концентрации и демассификации, лежащие в основе концепции сетецентрических операций.

4.7. Мягкая и жесткая модели ведения сетецентрических операций

В настоящий момент в области моделирования, планирования и реального осуществления сетецентрических операций и войн лидирующие позиции занимают США.

В качестве примеров можно привести практически все современные вооруженные конфликты и их участием, а также процедуры смены власти во многих государствах, начиная от

стран Латинской Америки и заканчивая нашими ближайшими соседями – Украиной и Грузией.

Существуют два основных типа моделей ведения сетецентрических войн: «мягкая» и «жесткая» (рис. 4.10.) Первые являются ***цветными революциями***, вторые – вооруженными конфликтами.

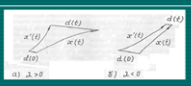
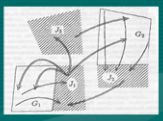
№	Сетецентрическая война	Нелинейная динамика	Иллюстрация
1	Мягкая форма развития ситуации (цветные революции).	**Метод управления "русел"** Русла – это где ход процессов предопределен, т.е. происходит плавный переход из системы в систему.	
2	Жёсткая форма развития ситуации (силовые решения).	**Метод управления "джокеров"** Джокер - это правило, в соответствии с которым объект в фазовом пространстве может совершить скачок. Это соответствует тому, что в таких системах есть два масштаба времени - "быстрый", на котором мы обычно не успеваем что-либо предпринять и "медленный", на котором в ряде случаев можно предотвратить аварию либо заняться ликвидацией ее последствий.	
3	Базовый эффект «ЛАВИНА»	**Эффект бабочки.** "Эффект бабочки" — незначительное влияние на систему может иметь большие и непредсказуемые эффекты где-нибудь в другом месте и в другое время	
4	Базовый эффект «ЭФФЕКТ РОЕНИЯ» «КОГЕРЕНТНЫЕ АТАКИ»	**Эффект когерентного усиления.** Помимо основного агрессора страну жертву атакуют сотни и тысячи общественных фондов и неправительственных организаций, щедро оплаченных и хорошо подготовленных. Большая часть из них очень слабо представляет стратегическую цель работы, которую они выполняют, а некоторые даже не подозревают о ее существовании.	

Рис. 4.10. «Мягкая» и «жесткая» модели развития ситуаций в ходе ведения СЦВ: аналогия ОБЭ и эффектов нелинейной динамики

4.7.1. Механизмы и инструменты «мягкого перехвата власти»

За последние десятилетия в мире накоплен богатый материал, позволяющий выделить манипуляционные модели технологий «ненасильственных» государственных переворотов, используемые в международной политике для свержения неугодных режимов. Бесспорный лидер в разработке и применении таких моделей - США. Долгие годы главным испыта-

тельным полигоном для этого скрытого геополитического оружия являлись страны Латинской Америки, Африки и, отчасти, Азии, где во второй половине XX в. США постепенно - по мере разработки новых глобальных манипуляционных моделей и их «шлифовки» - в основном перешли от довольно-таки грубой и непопулярной тактики смены неугодных им политических режимов с помощью прямых вооруженных агрессий или военных переворотов к решению этой задачи посредством организации массовых протестов и революций.

С конца 60-х гг. XX в. главным объектом использования таких моделей стали социалистические страны; первой из них была Чехословакия в 1968 г. После этого применение нового бескровного оружия в той или иной мере испытали на себе почти все социалистические страны, в том числе СССР. В последнее десятилетие модели глобального экологического манипулирования (включающие и скрытое программирование массовой психики) в форме «цветных революций» весьма эффективно использовались в Сербии, Черногории, Грузии, Украине, Киргизии, Ливане. В разных странах их называют по-разному: «революция красных гвоздик», «революция алых роз» и т.п.

Исследование технологий, применявшихся при организации «цветных революций», начиная с 2000 года, показывает, что спецслужбы США для достижения геополитических целей делают откровенную ставку как на «ненасильственных» способах свержения власти, так и их конкретном применении в «полевых условиях».

Обширный фактологический материал событий последнего десятилетия убедительно доказывает: «цветные революции» - это новая методика государственных переворотов, разработанная «мозговыми центрами» США совместно с ЦРУ[90]. Эти «революции», имевшие место в Сербии, Ливане, Киргизстане, на Украине, в Грузии, странах арабского мира – Туни-

[90] Оранжевые сети от Белграда до Бишкека» //Под ред. Н.А. Нарочницкой. Фонд исторической перспективы. - СПб.: Издательство «Алетейя», 2008 г.

се, Египте, Ливии, Йемене и др., и те, что не удались в Узбекистане, Армении, Беларусии преподносятся населению как народное волеизъявление. В действительности речь идет о хорошо организованных операциях, зачастую о преднамеренных постановках для СМИ, оплаченных и контролируемых транснациональными сетевыми организациями, которые также называют «неправительственными», и которые, в свою очередь, являются инструментами западного влияния. Используется весь арсенал средств воздействия - тайные операции, неявное, а в ряде случаев и явное применение военной силы, «черная» пропаганда, скрытое влияние и контроль, скупка ведущих журналистов, дезинформация в целях формирования общественного мнения в нужном ключе и иные методы, вплоть до политических убийств. Это и создание массовых оппозиционных движений, политических партий, широкое использование ИКТ в целях мобилизации больших масс населения, серьезные финансовые вложения в «революционную» атрибутику, акты индивидуального террора против неугодных представителей власти, создание вооруженных групп боевиков для подкрепления «мирных форм ненасильственного протеста», выдвигаемых под объективы западных телекамер, и многое другое.

Многие важнейшие аспекты технологий глобального психологического манипулирования анализируются в мировой и отечественной литературе. Данные технологии исследуются в первую очередь как «информационные войны», «психологические войны» и «коммуникативные технологии». Эти их аспекты (информационный, психологический, коммуникативный) чрезвычайно важны, однако недостаточны для раскрытия сути технологий глобального психологического манипулирования, которые включают целый комплекс аспектов, в том числе синергетический, организационный, экономический, микрополитический и др.

В основе моделей «цветных революций» лежат идеи синергетики и, в частности, идея ***эволюционного менеджмен-***

та[91] об использовании стихийных процессов самоорганизации для достижения желаемых целей. Этот подход предполагает анализ организационных процессов при управлении сетью, обеспечивающий всевозможные взаимосвязи элементов (сотрудников) и доступ их к любой информации по актуальной проблеме. Оказывается, что в социальных системах наиболее устойчивые и вместе с тем незаметные изменения происходят именно в результате стихийных процессов самоорганизации. Эти процессы складываются в результате согласования мнений и конкретных действий различных людей, движимых своими «частными» интересами и ценностями. Пример действия такого рода процессов - законы рынка, которые возникают без их осознания людьми как вектор, результирующая взаимодействия множества людей, преследующих свои эгоистические интересы.

Подобные стихийные процессы самоорганизации действуют и в политике. Их использование особенно эффективно для осуществления радикальных перемен в государственном устройстве. В частности, изменение государственного строя извне с помощью «механического» воздействия - интервенции, организации вооруженного мятежа и т.п. - гораздо менее эффективно, чем использование синергетического влияния. Чтобы, к примеру, устранить неугодного политика достаточно одного террористического акта. Свергнуть нежелательное правительство уже не так просто - нужна военная интервенция. Изменить же общественный строй еще сложнее - необходимо изменить самих граждан, обеспечить поддержку ими нового режима. Пока они будут считать навязываемый им порядок противоестественным, их сопротивление будет продолжаться или даже нарастать, и цели военно-политической акции не будут достигнуты. В этом проявляется общая закономерность **социокибернетики** - сконструированные в ре-

[91] Хиценко В.Е. Социальная самоорганизация и новая концепция управления. Новосибирский государственный технический университет.
http://www.lpur.tsu.ru/Seminar/a0100/a010400.htm

зультате внешнего, «механического» воздействия социальные системы сразу же распадаются, как только прекращается вмешательство их конструкторов (в данном случае страны-агрессора), люди восстанавливают привычные и желательные для них социальный порядок и уклад жизни.

4.8. «Цветные революции» как технологии передела власти в современной геополитике

Как было отмечено выше, о феномене «цветных революций» в публичном дискурсе российские эксперты впервые заговорили после событий в Сербии, Грузии и на Украине; затем аналогичные «революции» с разной степенью интенсивности последовали в Киргизии, Болгарии, Молдавии, Азербайджане, Армении, Узбекистане. Неудачная попытка провести цветную революцию по результатам выборов была предпринята в Белоруссии. Не обошли «революционные» настроения и Россию, так и не вылившись, однако, в активные массовые выступления. Эпидемия «цветных революций» охватила арабский мир - Египет, Тунис, Ливию, Бахрейн, Йемен, Ирак, Алжир. Попытка раскачать ситуацию с помощью технологий «народного волеизлияния и гнева» осуществляется с меньшей эффективностью в стабильных Сирии и Иране.

Сегодня геополитики активно изучают феномен «цветных революций», поскольку именно с их помощью происходит передел пространства власти в нестабильных регионах мира. «Цветные революции» ныне стали новейшим обретением политической технологии и высокой модой практики в борьбе за овладение властью.

Становится всё более очевидным факт, что по своей сути «цветная революция» - это спланированная смена режима с помощью психологической спецоперации по обработке граж-

данского населения под видом демократизации и в интересах западных стран.

Отличительный признак «цветных революций» - их тщательная спланированность и организованность. Их главная цель - смена геополитической ориентации государства, против которого направлена сетецентрическая операция на базе операций базовых эффектов (ОБЭ).

4.8.1. Сценарии цветных революций

Сегодня уже очевидно, что события цветных революций в большинстве случаев развиваются по одному и тому же шаблонному сценарию, который имеет некий общий первоисточник. Этот источник хорошо известен - книга американского политолога Джина Шарпа «От диктатуры к демократии»[92], которая была впервые опубликована в Бангкоке в 1993 г. Согласно Шарпу, политическая борьба в конституционных рамках против диктаторских режимов не имеет смысла, поэтому он предлагает демократической оппозиции целиком сосредоточиться на организации массового политического неповиновения властям.

В определенном смысле книга Шарпа представляет собой практическое руководство по захвату власти» - в ней излагаются тактика и стратегия борьбы оппозиции против тоталитарных и авторитарных режимов, а также наиболее действенные формы пропагандистской и организационной работы в различных социальных слоях населения, в том числе в армии и полиции. Неудивительно, что сегодня книгу Шарпа называют «библией» «цветных революций». [93]

---

[92] Джин Шарп. От диктатуры к демократии. Стратегия и тактика освобождения**.** Изд-во: Новое издательство, 2012

[93] См. Смирнов А.И., Кохтюлина И.Н. «Глобальная сила и «Мягкая сила 2.0»: вызовы и возможности для России.-М. ВНИИГеосистем. 2012.

Выделим основные этапы разработки возможного воздействия на сложную социальную сеть в рамках «мягкой» модели («цветных революций»).

1. Выявление конфликтного потенциала различных социальных групп на основе противоречий в интересах. Выделение социальных групп, политических объединений, способных стать стихийным инициатором (проводником) волны протеста.

2. На эту роль могут подходить «легко воспламеняемые» группы (например, молодежь). Поэтому на первый план здесь выходит анализ психологических особенностей групп или отдельных личностей (наиболее актуально в случае сравнительно малых масштабов сети, например, террористической организации).

3. Комплексная подготовка выделенных групп к дальнейшим активным действиям, определение концентраторов в рамках групп (в случае социальных сетей речь идет о дефакто лидерах, активистах).

4. Адаптация реальных целей в соответствии с мерой понимания выбранных групп и их концентраторов (возможно, навязывание ложных целей). Они должны быть уверены в практической осуществимости поставленных задач.

5. Обеспечение информационного превосходства навязываемых идей (использование СМИ, вбрасывание информации в целевую среду и т.д.).

6. Дальнейшее расширение контингента активных участников операции за счет обострения конфликтной ситуации («вербовка» новых «несогласных» элементов, повышение активности старых).

7. Оказание воздействий на систему защиты целевой сети с целью сокращения ее возможностей и, в идеале, полного блокирования.

8. Перевод целевой системы в бифуркационное состояние с возможным влиянием на ход ее дальнейшего развития.

9. После перехода системы в новое состояние (выгодное инициатору воздействий) ранее подогреваемые конфликты сводятся на нет, в том числе, с помощью «непопулярных» мер.

Теперь проанализируем основные особенности «жесткой» модели сетецентрического воздействия на сложную сеть.

1. Использование сетецентрических информационно-управляющих систем. Они обеспечивают высокую скорость управления функционированием своей сети в ходе активных деструктивных воздействий на сеть противника.

2. Обеспечение распространения информации в рамках своей сети в режиме, близком к реальному времени (доступность и своевременность).

3. Обеспечение конфиденциальности и целостности распространяемой по сети информации.

Заметим, что для решения практических задач наиболее актуально моделировать возможные воздействия на целевую сеть в рамках «мягкой» модели. В этом случае можно добиться желаемого эффекта и далее контролировать полученные результаты без необходимости обнаруживать свою активность в информационном поле.

4.8.2. Характерные черты «цветных» революций

Эксперты выделяют следующие отличительные черты «цветных революций»[94]:

- Использование преимущественно невоенных средств достижения целей - информационно-психологических воздействий, мирных политических акций, легитимных методов смены режима. Весьма благодатную почву для «цветных революций» представляют выборы, ведь необходимое условие бескровной революции - массовое участие в ней населения. Формой революции являются массовые митинги, демонстра-

[94] Пугачев В.П. Управление свободой. – М.: КомКнига, 2005.

ции и забастовки, которые проводятся оппозицией после проведения выборов, по результатам которых оппозиция объявляется проигравшей. Оппозиция в таком случае утверждает, что были допущены нарушения избирательного законодательства, исказившие волю народа. Массовые протесты приводят либо к проведению повторного голосования (Украина), либо к силовому захвату зданий органов власти толпой (Югославия, Грузия, Киргизия) и бегству руководителей государства с последующим проведением новых выборов. В обоих случаях оппозиция приходит к власти.

- Революция проходит под антикоррупционными и радикально-демократическими лозунгами. Ключевыми являются идеи народного суверенитета Руссо, где народ (сознательно вышедшие на улицу граждане) противопоставляется манипулируемой режимом массе.
- Революции предшествует формирование молодёжных организаций (Пора, Отпор и т. д.), которые образуют т.н. «полевые отряды революции».
- Революция носит подчёркнуто бескровный характер. Здесь отзвук движения Ганди и хиппи, которые раздавали полицейским цветы (*flower power*). Отсюда характерный бренд революции - неагрессивный цвет (не красный и не чёрный) или цветок. Однако в Киргизии в результате столкновений с полицией и погромов магазинов после силового захвата зданий органов власти толпой были пострадавшие (убитых не было). В Ливии также реальный сценарий развития революции пошел не по «шаблону», а привел к многочисленным жертвам.
- Решающую роль в успехе революции играет сдержанность силовых структур («не допустить пролития крови»).
- Некоторые говорят о связях уличных протестов с грантами или стипендиями таких фондов как фонд Дж.Сороса «Открытое общество», Гарвардский университет, институт Альберта Эйнштейна, Международный республиканский институт и Национальный демократический инсти-

тут (США), Международный центр ненасильственных конфликтов, Международный институт стратегических исследований в Лондоне и т.д.

- Проамериканская политика после революции - даже если считать, что прямых действий со стороны США, в виде денежной и консультационной помощи, не было, сложно отрицать факт, что после цветных революций политический курс становился подчёркнуто проамериканским, иногда построенным на антироссийской риторике. В свою очередь, США открыто поддерживает эти режимы. Наиболее яркими представителями такой политики являются Грузия и Украина. Учитывая сильные экономические связи с Российской Федерацией, особенно у Украины, это приводит к регулярным сбоям в торговых отношениях и, косвенно, приводит к ухудшению экономического положения таких стран.

Так, например, финансируемая рядом стран Запада «Политическая академия Центральной и Юго-Восточной Европы» в Болгарии учредила программу для подготовки сербской оппозиции. Еще одна болгарская организация - «Балканская академия старших репортёров» - предоставляла «финансовую, техническую и экспертную помощь» югославским оппозиционным СМИ перед выборами. Организация «Новый сербский форум» обеспечивала регулярные поездки сербских специалистов и студентов в Венгрию для «бесед и консультаций» с западными экспертами. «Национальный фонд поддержки демократии» (США) курировал сразу две неправительственные американские структуры в регионе - «Международный республиканский институт», делавший ставку на работу с оппозиционными партиями, и «Национальную демократическую организацию», обучившую с 1997 по 1999 годы свыше 900 лидеров и активистов правых партий «предвыборной стратегии и умению привлекать широкое внимание».

Значительные финансовые ресурсы на организацию «цветных» революций поступали через американский фонд

«Поддержки демократии в Восточной Европе» (Support for East European Democracy - SEED). Расходы SEED - часть бюджета госдепартамента США. Общие финансовые поступления через SEED только в Сербию составили: в 1998 году - 15,3 млн долларов, в 1999-м - 24,3 млн долларов и в 2000-м - 55 млн долларов. Для их распределения использовались, в частности, каналы организации «Балканская инициатива» при Американском институте мира. В украинскую «оранжевую революцию» США вложили более 85 млн. долл. Дж.Сорос, выступая в начале 2004 г. на экономическом форуме в Давосе, весьма откровенно признался, что именно на его деньги грузинские деятели «революции роз» свергали обанкротившегося «белого лиса» (Эдуарда Шеварднадзе). «Я горжусь совершенной в Грузии революцией», - заявил Сорос и пообещал, что его фонд поможет Саакашвили и в дальнейшем. Всего же в период правления Джорджа Буша США потратили на поддержку «демократических изменений» около 5 млрд. долл.

- Формирование символа. Выступает важным элементом техники и методов осуществления бархатных революций, а также является своеобразным средством общения и идентификации единомышленников. В Сербии это был сжатый кулак, на Украине - оранжевый цвет, в Грузии - роза, в Киргизии - тюльпан. Обязательным качеством любого символа должна быть узнаваемость и несложная возможность его нанесения различными способами в общественных местах.
- Кампания неповиновения власти. Состоит в организации массированного давления на органы исполнительной власти на различных её уровнях. Формами такого давления, как правило, выступают митинги и забастовки всех видов, голодовки, представление поддельных документов, блокирование информационных линий и транспортных коммуникаций, снятие указателей госучреждений, бойкот выборов, отказ от уплаты налогов, отказ от должности и работы с правительством и т. д.

- Главная ударная сила «цветной революции» - не революционное большинство народа, а так называемая «пятая колонна», финансируемая из-за рубежа.
- В отличие от традиционных, «**цветная революция» - это сетевой процесс**, работающий по сетевому принципу и активно использующий все каналы СМИ для легитимации своих целей и задач.
- Еще одним условием развития революции является **мобильность и сетевой принцип деятельности**, умелая работа с предметно-целевыми группами населения, ключевыми с точки зрения коммуникации, создания необходимого общественного фона (молодежь, женщины, интеллигенция, таксисты, работники газетных киосков и т.д.).

Таким образом, в определенном смысле «цветные революции» можно рассматривать как **особую форму информационной войны.** Весьма важно определить причины, генерирующие данный феномен. Сегодня ни для кого не секрет, что главным катализатором «цветных революций» становятся внешние факторы и ресурсы. **Необходимым условием осуществления таких революций является наличие активных зарубежных спонсоров, финансирующих молодежные организации и оппозиционные политические партии, лидеры которых заявляют о своей поддержке западной модели демократии.** Вполне очевидна связь активистов революций с грантами или стипендиями таких организаций, как Институт «Открытое общество» (Фонд Джорджа Сороса), Гарвардский университет, Институт Альберта Эйнштейна, Международный республиканский институт и Национальный демократический институт (США), Международный центр ненасильственных конфликтов, Международный институт стратегических исследований в Лондоне и многих других.

Таким образом, можно констатировать, что у «цветных революций» в разных странах есть общее координирующее начало - Вашингтон. Там определяют как будущее уже побе-

дивших цветных революций, так и страны-кандидаты на очередную «цветную революцию».

Во многом катализатором «цветных революций» становится недовольство действующей властью на фоне серьезных социально-экономических проблем, поэтому страны с затянувшимся экономическим переходным периодом составляют в этом отношении главную «группу риска». Экономисты предупреждают: если в стране только 20% людей вписалось в рыночную экономику, это опасно и может в любой момент привести к тому, что в обществе начнется социальный раскол.

Другим катализатором цветных революций является слабость действующей власти, которая даже в критических условиях декларирует свою приверженность демократическим ценностям и идеалам. **При этом международная общественность всячески поддерживает «демократическую» пассивность власти (например, в рамках «Евромайдана» в Украине), кроме того, проводится определенная программа по блокировке силовых решений.** Это прекрасно видно на примере стран СНГ, лидеров которых последовательно уводили как от решительных действий, так и от борьбы в целом. Не случайно революции происходили в самых демократических странах СНГ. Например, Украина и Грузия обладали достаточной свободой СМИ, Киргизия имела одного из самых демократичных в своем регионе президента.

Наконец, особым катализатором «цветных революций» выступают средства массовой коммуникации, что позволяет говорить об эффекте «эфирократии». Через информационные потоки идет процесс активных политических манипуляций общественным мнением, чтобы представить революцию как «победу сил демократии». При этом информационные технологии направлены, прежде всего, на то, чтобы придать толпам на улицах статус «народа». Именно каналы мировых СМИ гарантируют митингующим статус «революционного авангарда», гордо вышедшего на авансцену истории.

4.8.3. Роль СМИ при подготовке, проведении и достижении базовых эффектов «цветных революций»

Кризис в странах-жертвах искусственно разжигается и поддерживается ангажированными СМИ, которые непрерывно заполняют информационное пространство хаотическим потоком сообщений и комментариев, способствуя тем самым усилению социальной неустойчивости. В информационном пространстве формируется **виртуальная реальность,** позволяющая генерировать изменения в других областях человеческого общества. Изменяя виртуальные артефакты в нужном направлении, мы получаем соответствующие результаты в подлинной реальности, причем влияние этих артефактов резко возрастает в момент бифуркации, когда неопределенность порождает острую потребность в новой социальной информации. *В результате усиливается зависимость кризисного общества от информационной и особенно виртуальной реальности, где фабрикуются различные версии, схемы и доктрины грядущего общественного переустройства, которые вряд ли станут объектом рационалистического интереса со стороны основной массы населения, равнодушного к идеологическому дискурсу.* В условиях социобиологической борьбы людей за свое собственное выживание восприятие информации носит эмоциональный и бессознательный характер, и потому оценка социальной утопии, противостоящей старому идеологическому канону, не может не быть тенденциозной и пристрастной.

В период бифуркации социума действует отчетливая закономерность: чем нестабильнее состояние кризисного общества, тем сильнее суггестивное[95] воздействие СМИ на массовое сознание.

[95] Суггестивный - воздействующий на чьи либо мысли, подсознание или поведение; (психол.) основанный на внушении, гипнозе.

Действительно, люди, которые неожиданно оказались в условиях неопределенности, пытаются адаптироваться к ней, что усиливает их зависимость от новой информации и, значит, СМИ. Кризис общества побуждает средства массовой коммуникации транслировать альтернативную информацию, чтобы найти новые идеи общественного переустройства. Новая информация неизбежно меняет картину мира, что, в свою очередь, может мотивировать получателей информации на изменение реального социального мира, с тем, чтобы последний соответствовал созданной **виртуальной действительности.** *Возникает неустойчивая ситуация, которая способствует тому, что реальный социальный мир трансформируется сообразно виртуальной картине мира.* Информационная составляющая кризисного общества обладает достаточно большим потенциалом воздействия на процесс социетальной трансформации, стимулируя изменения не только в информационном поле, но и в других значимых полях. Набор различных задач, акгуальных с точки зрения смены социетальной системы, предполагает активизацию информационной составляющей, поскольку структуры власти, находящиеся под контролем старой элиты, можно наиболее эффективно дезавуировать с **помощью** символического насилия. Как отмечает П.Бурдьё, «познание социального мира, точнее, категории, которые делают социальный мир возможным, суть главная задача политической борьбы, борьбы столь же теоретической, сколь и практической, за возможность сохранить или трансформировать социальный мир, сохраняя или трансформируя категории восприятия этого мира»[96]. Под влиянием символической войны власть утрачивает свой господствующий статус, поскольку новая социальная информация разрушает легитимность старой системы господства и подчинения. Контрэлита интенсивно трансформирует старое мировоззрение, внедряя в общественное сознание новую картину мира, соответствую-

[96] Бурдье П. Социология политики. М,, 1993. С. 66.

щую цели и задачам системного преобразования кризисного социума.

4.8.4. Социальная сеть микроблоггинга Twitter: «Twitter-revolution» - главный инструмент «цветных революций»

В последние годы влияние Интернет-технологий на политические процессы во всем мире привлекает все большее внимание исследователей. Тому есть объективные причины - ни одна из недавних «цветных революций» в постсоветских странах, а также в странах арабского мира не обошлись без активного использования новейших коммуникационных средств. Наравне с общеизвестными уже блогами (типа LiveJournal), социальными сетями (Facebook) и видеохостингами (YouTube), признание в качестве «инструмента политики» получила и социальная сеть микроблоггинга Twitter[97]. Та огромная роль, которую Twitter сыграл во время упомянутых уже «цветных революций», заставляет присмотреться к данному сервису поближе. К слову, в зарубежных СМИ даже появился специальный термин - «Twitter-revolution».

Согласно соцопросам, накануне выборов в Молдавии в апреле 2009 года поддержка партии коммунистов во главе с президентом республики Владимиром Ворониными составляла не более 35%. Когда же огласили официальные данные, эта цифра возросла до 50%. Мобилизованные путем рассылки сообщений в социальной сети Facebook, а также призывов в

[97] Социальная сеть микроблоггинга Twitter появилась в 2006 году и всего за несколько лет приобрела огромную популярность в мире. Согласно отчету исследовательской компании comScore, аудитория Twitter в январе 2010 года составила 73,5 млн пользователей. Twitter - это программа, позволяющая публиковать в Интернете небольшие сообщения, доступные для чтения большому количеству людей. Отправлять их можно с помощью мастера отправки мгновенных сообщений, SMS, RSS, E-mail и пр. Краткость сообщения (всего 140 знаков) составляет одну из отличительных черт микроблогов и их же главное преимущество: оперативность. Собственно, оперативность и стала главной причиной использования Twitter во время «цветных революций» и массовых протестов.

Twitter, на улицы Кишинева вышли тысячи молодых людей. Начались стихийные митинги и демонстрации, а позже - грабежи, погромы, поджоги. С самого начала демонстраций оппозиционные силы создали свой собственный ярлык поиска в сети Twitter - #pman (означает «Пяца Марий Адунэрь Националe» - центральная площадь Кишинева), на котором публиковались новости о развитии событий. Под хештегом #pman публиковались призывы оппозиции к объединению, сведения о действиях властей и полиции, данные о местах акций протеста, фиксировалось количество пострадавших от рук полиции. Таким образом, благодаря Twitter, оппозиционные силы умело координировали свои действия. После того, как власти блокировали сотовую связь в столице, протестующие использовали GPRS-связь (мобильный интернет) для публикации своих сообщений. «Обновления на Twitter публиковались в рекордные сроки - пишет сотрудник института Открытого общества Евгений Морозов. - Я смотрю на поток последние 20 минут и вижу почти 200 новых сообщений, маркированных #pman…». Помимо непосредственно текстовых сообщений, записи содержали также многочисленные ссылки на видео, содержащееся на видеохостинге YouTube. Видео снимали сами протестующие при помощи камер на мобильных телефонах. Многие посты специально печатались на английском языке, чтобы быть прочитанными зарубежными журналистами.

События, происходившие в Молдавии, спустя несколько месяцев повторились в Иране. «Спусковым крючком» для оппозиции снова стало несогласие с результатами выборов - на этот раз президентских. Начались акции протеста против результатов голосования. Сторонники оппозиционного кандидата Мир-Хоссейна Мусави поджигали здания банков, полиции, громили проправительственные информагентства. Помимо полицейских рейдов, ответом властей на протесты стала глубокая информационная блокада. С самого дня выборов в стране оказалась заблокирована служба SMS-

сообщений, сотовая связь, большинство социальных сетей, блогов. Сигналы иностранных радиостанций глушились, с домов снимали спутниковые антенны. Государственное телевидение не показывало демонстрантов, зато в телесюжетах говорилось о беспорядках, устроенных иностранными агентами.

И снова, по сути, главным информационным ресурсом протестующих стал мобильный интернет и сайт Twitter: практически каждую секунду появлялись сообщения о подготовке акций, ссылки на фотографии митингов и списки арестованных, советы, как зайти на заблокированные сайты, а также предупреждения, где в Тегеране собрались полицейские. Зарубежные СМИ с воодушевлением восприняли Twitter-революцию в Иране: «В этом году иранской инновацией стало быстрое распространение свежей информации и использование технологий коммуникации. Детали демонстраций, тактика, лозунги - все распространяется в Twitter… Видео выступлений и сцен стрельбы выкладывается на Youtube и подобных сайтах - и их можно скачать из-за пределов Ирана и потом извне транслировать обратно на эту страну с помощью средств массовой информации».

Ответной акцией властей на сообщения в Twitter стало большое количество подставных агентов, публиковавших в сети микроблоггинга ложные сообщения. В свою очередь, протестующие распространили в Twitter текст под заголовком «Кибер-война против иранских выборов для начинающих», для того чтобы помочь остальным участвовать в сетевых протестах. Пособие содержало советы, как сделать так, чтобы спецслужбы не узнали пользователя по логину и IP-адресу, а также как вычислить правительственных агентов, скрывающихся в Twitter под видом оппозиционеров.

В Иране посредством Twitter распространялись также ссылки на специальную компьютерную программу («Митбот»), предназначенную для организации кибер-атак на проправительственные интернет-сайты. Скопировав подобную

программу на свой компьютер, пользователь получал возможность посылать многочисленные запросы на целевые вебсайты. Подобный способ взламывания сайтов за счет их перегрузки получил широкое распространение и называется DDoS-атакой. Кибер-атаки во время иранских событий были названы в СМИ единственным оружием борьбы общества против информационной цензуры. Таким образом, Twitter стал ареной полномасштабной информационной войны.

После описанных событий в Молдове и Иране власти некоторых стран, в частности, Южной Кореи, стали ограничивать в дни выборов использование Twitter. По требованию южнокорейского центризбиркома, во всех записях в Twitter, касающихся предвыборной кампании, теперь должно стоять указание, что это агитация. В избирательном законодательстве, на которое ссылаются власти, запрещается в целях пропаганды одной из партий использование постеров, печатных материалов, видеороликов и т.п. Иными словами, Twitter фактически приравнен в Южной Корее к СМИ.

Интернет стал также одним из самых действенных средств организации массовых беспорядков в ходе «жасминовой» революции в Тунисе, закончившихся падением действующего режима и бегством из страны президента Зин аль-Абидин бен Али, который правил Тунисом с 1987 года. Благодаря Интернету, с самых первых дней беспорядков по всей стране распространялись требования манифестантов, живые картинки уличных событий и, в первую очередь, жестокость полицейских и солдат - все это немедленно становилось известно всем подключенным к Сети. Власти отрицали, что в ход пущены слезоточивые газы, - Интернет тут же это опровергал. По государственному радио вещали, что «ситуация под контролем правительства», а в режиме онлайн шло совсем другое. Властям не удалось скрыть ни размах выступлений, ни репрессии. Еще раз было доказано: Интернет - сила, способная пробить стену молчания, которую пытается возвести теряющий поддержку режим.

Ряд авторитетных американских изданий, включая газету New-York Times и журнал Foreign Policy, высказали неожиданную версию: падение режима Зина аль-Абидина бен Али в Тунисе могло спровоцировать появление на сайте WikiLeaks конфиденциальной информации.

По мнению автора статьи, появление в открытом доступе секретной дипломатической переписки стало своего рода спусковым крючком и послужило одной из причин массовых беспорядков и погромов в стране. «Эти телеграммы, которые удалось добыть и... обнародовать организации WikiLeaks, способствовали тому, что гнев народа выплеснулся на улицы и достиг своей кульминации в пятницу, когда бен Али, на протяжении 23 лет остававшийся у власти, вынужден был покинуть страну», - поясняется в публикации. В журнале Foreign Policy, в свою очередь, говорится: «Разумеется, народ Туниса и сам давно знал об этом. Но изложенные в депешах подробности - например, то, что жена президента присвоила крупные средства, которые правительство выделило на поддержку ее частной школы, - дополнительно подогрели страсти. Власти закрыли гражданам Туниса доступ к WikiLeaks и начали вылавливать в социальных сетях диссидентов и активных оппозиционеров, однако данные меры не улучшили, а, напротив, ухудшили обстановку в стране».

Несмотря на очевидные преимущества, которые Twitter вкупе с другими современными Интернет-сервисами дает участникам политических протестов (революций), не следует переоценивать его возможности. В частности, оценивая итоги «оранжевой революции» на Украине (в ней решающая роль, правда, отводилась не Twitter, а мобильным телефонам)[98], Евгений Морозов пишет: «Ошибка считать, как это делается в некоторых последних исследования центра Беркмана, что «оранжевая революция» была делом «умных толп»... Фокусировать внимание только на технологии - значит, не обра-

[98] В ходе кризиса на Украине 2013-2014 гг. социальные сети, в т.ч. сеть микроблогов «Twitter», использовались очень активно – подробнее в главе 5.

щать внимания на попытки сфальсифицировать результаты президентских выборов, что и вызвало протесты... или на миллионы долларов, «вкачанные» в украинские демократические силы, чтобы протесты стали возможными... То, что режим меняется благодаря текстовым сообщениям, может казаться реалистичным только в цифровом пространстве. Кроме того, давно уже не является секретом истинный механизм «цветных революций» и ненасильственных переворотов. «Цветные революции» отличаются подчеркнуто коммуникативным характером. Это новый тип давления - информационный, создающий информационно-организационный тип революции, которого никогда не было ранее...».[99]

Во время «цветной революции» **информация выполняет следующие функции**:

- формировать и активизировать массовое сознание, удерживать своих сторонников в активном состоянии до победы;
- легитимизировать «революционные» действия для внутренней и внешней аудитории;
- устрашать оппонентов для недопущения применения ответных активных действий;
- легитимизировать новых лиц в качестве руководителей.

Добавим сюда координацию действий участников протеста - как видим, возможности Twitter органично вплетаются в общую теорию ненасильственных переворотов. Таким образом, можно заключить: **социальная сеть микроблоггинга Twitter играет важную, а подчас и решающую роль в организации современных политических протестов**. Сервис используется для координации действий участников протестов, привлечения внимания зарубежных СМИ к проблемам региона, публикации лозунгов оппозиции и нагнетания информацинного давления. Кроме того, Twitter может являться

[99] Лада Браславец. Социальная сеть микроблогов «Twitter» как среда распространения массовой информации//www.relga.ru, №14 [194] 01.10.2009

своеобразной «платформой» для передачи ссылок на видеодокументы (снятые, в свою очередь, при помощи мобильных телефонов), различные материалы СМИ, а также программы для организации кибер-атак. Следует признать, что наибольшего эффекта Twitter достигает именно в совокупности с различными интернет-сервисами - Facebook, YouTube, Livejournal и пр., обладая при этом важнейшим отличием от них - практически неограниченной оперативностью. Использование Twitter, однако, в большой степени зависит от «подготовки почвы» для протестных действий или прочих коллективных акций. «Твиттерная революция-2009» в Иране провалилась. Но «революционные порывы» вновь сотрясают эту страну. И опять же во всю мощь задействованы информационные технологии: Госдепартамент США завел на Twitter.com микроблог на фарси, чтобы обращаться к иранцам. В этих сообщениях - обвинения в адрес иранского руководства. Сетевое наступление активно идет и на другие страны региона.

В целом же, очевидно: Twitter обладает гигантским потенциалом с точки зрения развития социального моделирования. Глубоко не случайно, что после отставки Мубарака в обстановке строгой секретности Обама отужинал с главами крупнейших высокотехнологических компаний мира: Facebook (глава - *Марк Цукерберг*), Google (глава - *Эрик Шмидт*), Twitter, Yahoo!, NetFlix, Oracle. На «тайную вечерю» вытащили даже умиравшего от рака шефа Apple Стива Джобса.[100] Хиллари Клинтон заявила, что Госдепартамент выделяет серьезные дополнительные средства на «поддержку технических экспертов и активистов, старающихся действовать в обход ограничений, устанавливаемых правительствами в отношении доступа к Интернету».[101]

[100] Евгений ЧЕРНЫХ. Америка развязала Первую мировую сетевую войну? Сможет ли Россия противостоять электронным атакам? //Комсомольская правда, 03.03.2011.
[101] Евгений ЧЕРНЫХ. Америка развязала Первую мировую сетевую войну? Сможет ли Россия противостоять электронным атакам? //Комсомольская правда, 03.03.2011.

Интернет становится полигоном для отработки и других новых технологий «социального конструирования» якобы произвольных, официально не инициированных извне «сетевых революций» в тех или иных государствах, заканчивающихся, в конечном итоге, отнюдь не виртуальным исходом, а мобилизацией критической массы молодежи для ультимативной реакции на действия властей, создания массовых беспорядков и падения режимов в этих странах. К таким инструментам относятся «троллинг» и «астротерфинг».

Тро́ллинг (от англ. *Trolling* - блеснение, ловля рыбы на блесну) - размещение в Интернете (на форумах, в дискуссионных группах, в вики-проектах, «живых журналах» и др.) провокационных сообщений с целью вызвать противоречия и конфликты между участниками, взаимные оскорбления и т.п. Лицо, занимающееся троллингом, называют *троллем*, что совпадает с названием мифологического существа.

Слово «троллинг» может характеризовать либо непосредственно одно сообщение, либо в целом размещение таких сообщений. Также под «троллингом» часто подразумевается психологическая манипуляция, основанная на публичном высмеивании или уничижении убеждений (в основном заблуждений или предубеждений, радикальных взглядов и т.д.) оппонентов, приводящая к эмоциональной нестабильности последних (эмоциональным срывам в той или иной форме, проявление которых называется «заглотнул блесну» и обычно является конечной целью «троллинга»). Понятие «троллинг» также используется, чтобы описать деятельность Интернет-хулиганов вообще. Троллинг - игра в подделку личности, но без согласия большинства игроков, не сознающих участия в этой игре. Тролль пытается зарекомендовать себя как типичный пользователь, разделяющий общие интересы и проблемы группы.

Интернет-тролли стали образовывать собственные сетевые сообщества и организации, делясь опытом по наиболее эффективному разжиганию конфликтов. Сейчас любой попу-

лярный форум, группа новостей и вики-проект рано или поздно сталкивается с троллями и троллингом. Высшей целью тролля является возможность получить права на редактирование терроризируемого им форума и управление им. Тролль-модератор, занимаясь троллингом, прикрывается так называемыми «функциями модератора», заключающимися в слежении за соблюдением порядка на его усмотрение. Администратором (супермодератором) форума стать гораздо сложнее, для этого необходимо личное доверие создателя форума (или самому создать форум изначально для цели троллинга), но в случае успешного достижения троллем этого статуса (либо превращения действующего администратора или создателя форума в тролля) форум-сообщество практически обречено. Однако PR-троллинг может являться средством поднятия рейтинга сайта и его целью может быть удержание пользователей сайта в острой дискуссии, тем самым привлекая новых пользователей.

Следует также отметить, что помимо чисто субъективных проявлений, троллинг взят на вооружение спецслужбами и бойцами информационных войн. В этом случае цель применения троллинга - это, в частности, отвод внимания от острых тем и превращение конструктивного обсуждения в перепалку. Одним из методов нападения является агрессивный вброс клеветы, компромата, слухов и т.д.

Другой формой контроля за сетевыми сообществами стал так называемый «**астротерфинг»** (от англ. **AstroTurf** - искусственная трава для спортивных площадок) - механизм создания искусственного общественного мнения. Или, если быть совсем точным - имитация «общественного мнения» нужной направленности (то есть население заменяется на ботов, которые и высказываются нужным образом)[102]. Термин появился по аналогии с более старым PR-термином **Грассрутинг (**от англ. **Grassroots –** корни травы**)** - подразумевающим **вы-**

[102] Боты атакуют! **(**http://bohn.ru/news/boty_atakujut/2011-03-02-187**)**

ращивание необходимого общественного мнения снизу (примерно так, как растят траву на газоне - накидать семян, потом поливать и удобрять).

Впервые этот метод был реализован MOSSAD, который начинал с того, что подряжал русскоговорящих израильских студентов торчать на русских форумах под видом граждан России, и «отстаивать там линию Израиля». Собственно, именно тогда были сделаны первые заделы по «**persona management software**» для оперативной регистрации множества личин на разных ресурсах и переключения между ними.[103]

Анонимность Интернета дает компаниям и правительствам блестящие возможности для астротерфинга - фальшивых массовых кампаний, создающих впечатление, будто масса народу требует определенного политического курса либо выступает против него. Специальные программы - так называемый «persona management software» - создают весь антураж, который есть в онлайне у реального человека: имя, почтовый ящик, сайты, аккаунты в соцсетях. Особое беспокойство участников социальных сетей вызывает то, что этот инструментарий привлек особое внимание военных и специальных служб. Так, ВВС США объявили тендер на поставки комплекса специальных программ «persona management software», которые могут создавать «10 личин для одного пользователя», снабжать астротерферов выбранными наугад IP-адресами, а также создавать статичные IP-адреса для каждой личины, чтобы астротерферы могли поочередно выступать от ее лица[104].

Такой активно продвигаемый инструмент, будучи анонимным, дает возможность целенаправленной дискредитации личности оппонента, травли его и его близких, подавления государственных Интернет-порталов, целенаправленного формирования общественного мнения. По сути дела речь

[103] Об аналогичном опыте Госдепа и разведсообщества США в главе 8.
[104] http://inopressa.ru/article/28Feb2011/g ... ernet.html

идет о создании системы рефлексивных управляемых событий посредством «социальных сетей». События на Ближнем Востоке и в Северной Африке являются достаточно убедительным аргументом в пользу констатации очевидного фактора использования социальных сетей для организации массовых деструктивных «протестных выступлений», заканчивающихся той или иной формой «цветной революции».

Зная о том, какие шаги предпринимают США, России необходимо мобилизовать свой научно-технический и интеллектуальный потенциал для создания асимметричного потенциала способности ведения глобального информационного противоборства на основе новых информационно-коммуникационных технологий ГИР, Web 2.0 и облачных вычислений с целью обеспечения собственной информационной и, как следствие, национальной безопасности.

Резюмируя, следует подчеркнуть, что:

- Практическая отработка США концепции ведения СЦО на реальных полигонах управляемых военных конфликтов, «миротворческих операций» (в том числе и без мандата ООН) и инспирированных «цветных революций» с целью установления геополитического доминирования в XXI веке означает фундаментальную смену парадигм управления вооруженными силами от «платформоцентрической» к «сетецентрической».
- Перевод боевых действий в 5-ое информационное измерение создает принципиально новую глобальную угрозу установления мировым гегемоном (и силами за ним стоящими) управляемых вассальных режимов потенциально в любой стране-жертве и достижение синергетического эффекта ее экономического подчинения без ведения войны путем покрытия ее паутиной экономических, военно-политических, дипломатических, торговых, социально-ориентированных и др. обязательств, принуждений, воздействий и рефлексий.
- «Холодная война» в новой сетевой редакции ведется на новых фронтах: культурном, цивилизационном, этниче-

ском, религиозном и т.д. Эта война является по содержанию духовно-борческой, по сути - сетевой, а по организации - сетецентрической.

- «Холодная война» против СССР в настоящее время трансформировалась в глобализационное противостояние США с Россией и остальным миром и имеет свойство тотальности нескрываемых, и даже открыто декларируемых целей по установлению полной монополии на власть на планете по сценарию Pax America.
- Основным критерием для прогнозирования мероприятий и кампаний, направленных на дестабилизацию общественно-политической ситуации и рост социального противостояния в России, является уровень проникновения в регион структур влияния «сетевой войны» в виде тех или иных НПО, формальных и неформальных, и имеющейся в их распоряжении ресурсной базы (материальной, людской, интеллектуальной, информационной, административной).
- Размывание традиционных ведомственных границ и переплетение сфер ответственности оборонных, разведывательных, дипломатических и правоохранительных структур (а в определенном смысле - и границ публичной и частной сфер) - ключевые следствия новых вызовов общественной и государственной безопасности в эпоху информационно-коммуникативной революции.

Неизбежность вышеуказанных процессов становится все более очевидной с учетом фактора сетевой войны и императивно требует системного, в т.ч. институционального реагирования.

Нам не дано предугадать.
Как слово наше отзовется, -
И нам сочувствие дается.
Как нам дается благодать.

Ф.И.Тютчев

5. ВИРТУАЛЬНЫЙ «УКРАИНСКИЙ ФРОНТ»

5.1. Евромайдан 2.0 (попытка краткого генезиса)

Майда́н Незале́жности (укр. Майдан Незалежності - разговорный вариант «Майдан»; означает «Площадь Независимости») - центральная площадь Киева.

В XXI веке площадь стала местом протестных акций: зимой 2000-2001 гг. «Украина без Кучмы», в 2004 г. - Оранжевой революции, как одной из инспирируемых извне «цветных революций».

Ора́нжевая револю́ция (укр. Помара́нчева револю́ція от укр. помара́нчевий - оранжевый) началась после 21 ноября 2004 г., когда Центризбирком Украины объявил предварительные результаты президентских выборов: с преимуществом в 3 % победил В.Янукович (в то время премьер-министр). Сторонники соперника Януковича на выборах - В.Ющенко, и большинство иностранных наблюдателей считали, что этот перевес был достигнут за счёт нарушений на выборах.

3 декабря 2004 г. Верховный Суд Украины признал, что определить победителя не представляется возможным, и, вопреки законодательству, назначил переголосование на 26 декабря 2004 года. Повторное голосование зафиксировало победу Ющенко с отрывом в 8 %.

Политический кризис на Украине (2013-2014) разразился после решения правительства 21 ноября 2013 г. приостановить процесс подписания Соглашения об ассоциации с ЕС.

По словам премьера Азарова «последней каплей» послужило письмо МВФ, в котором Украине для получения кредита предписывалось повысить тарифы на газ и отопление на 40%, заморозить зарплаты и сократить бюджетные расходы. Кроме того, в результате евроинтеграции около 400 тыс. украинцев могли оказаться без работы[105]. Азаров подчеркнул, что приостановка процесса евроинтеграции является тактическим ходом и не связана с отказом от прежнего курса.

Когда он заявил, что в качестве альтернативы выполнению условий МВФ правительство взяло курс на восстановление экономических отношений с Россией[106], оппозиция в раде устроила ему обструкцию.

5.1.1. От поста в Facebook к государственному перевороту

Решение о приостановке евроинтеграции привело к массовой акции протеста в центре Киева, а также в других городах Украины, получившей в соцсетях и СМИ название «Евромайдан» по аналогии с событиями 2004 г.

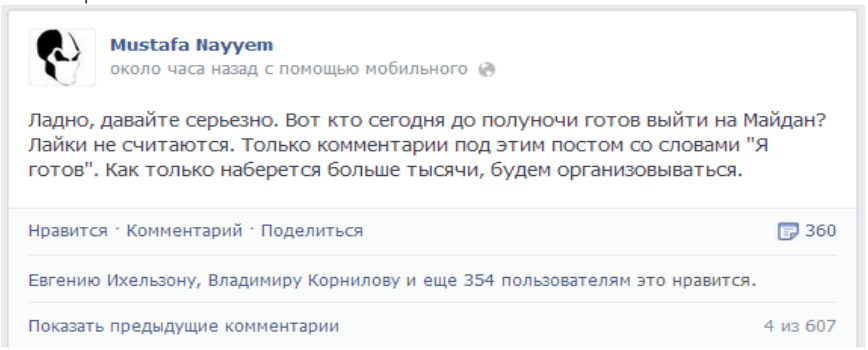
Её стартом можно считать пост известного украинского блогера Мустафы Найема (афганского происхождения), который призвал в Facebook выйти на Майдан 21 ноября 2013 г.[107]

[105] http://glavred.info/ekonomika/azarov-obyasnil-otkaz-ot-associacii-400-tysyach-ukraincev-mogli-poteryat-rabotu-264530.html 11.06.2014

[106] 10 октября украинские коммунисты инициировали сбор подписей против евроинтеграции и за вступление в Таможенный союз ЕврАзЭС. За 40 дней им удалось собрать 3,5 млн подписей в поддержку референдума.

[107] Мустафа Найем (Mustafa Nayyem) стал первым в Украине пользователем Facebook, которого читает свыше 100 тысяч человек. При этом с ноября 2013 г. он прибавил свыше 70 тысяч новых читателей.
https://www.facebook.com/profile.php?id=1414642146 15.05.2014

21:22 | 20 хвилин



Через час после публикации, количество комментариев перевалило за 600, а желающих выйти на Майдан - более тысячи. Позже появилось сообщение: «Встречаемся в 22:30 под монументом Независимости…».

Практически все участники акции постоянно находись в виртуальном мире: переписывались в соцсетях, выкладывали видео и фото файлы, приглашали к протестам друзей и знакомых по всей Украине. Как уже отмечалось в предыдущей главе по аналогии с другими «цветными революциями» в качестве причин протестов в соцсетях активно муссировали социальную несправедливость, огромную поляризацию доходов и уровня жизни населения Украины и разгул коррупции.

На майдане собирались десятки тысяч участников с музыкой, страстными речами, романтическими подсветками экранами мобильных телефонов. Шел мирный этап протеста, или «Евромайдан 2.0».

Однако после Вильнюсского саммита «Восточного партнёрства» (28-29 ноября 2013 г.), разгона палаточного городка оппозиции на «Евромайдане» и принятия 16 января 2014 года Верховной радой законов по ужесточению санкций за участие в массовых беспорядках протесты резко обострились.

Для защиты «Евромайдана» националистические группировки (УНА-УНСО, «Тризуб», «Патриот Украины» и др.) составили праворадикальное объединение «Правый сектор»,

считавшее Евромайдан лишь удобным поводом для начала «национальной революции». Характерно, что «Правый сектор» с самого начала координировал свои действия через социальные сети. Его рупорами стал сайт «Бандеравец»[108], а также страницы в сетях Facebook и Vkontakte.

Силовое противостояние в Киеве, захват зданий и органов власти в столице и областных центрах, создание параллельных органов власти, организация неформальных силовых структур поставили Украину на грань введения чрезвычайного положения, утраты территориальной целостности и экономического коллапса.

Переговоры между президентом Януковичем и лидерами оппозиции привели к уступкам властей: было созвано внеочередное заседание Верховной рады, проголосовавшей за отмену ряда законов и принявшей закон об амнистии участников акций протестов, была принята отставка премьера Азарова. Янукович согласился на формирование коалиционного правительства.

В то же время 16-17 февраля 2014 г. ВО «Майдан» и «Правый сектор» объявили о подготовке «мирного наступления» на Верховную раду (одновременно Яценюк и Кличко совершили поездку в Германию для консультаций с канцлером Ангелой Меркель). На следующий день произошло резкое обострение ситуации с массовым кровопролитием.

21 февраля под давлением стран Запада Янукович пошёл на уступки и подписал с оппозицией (с участием мининдел ФРГ, Польши и Франции) соглашение об урегулировании кризиса на Украине, предусматривавшее, в частности, немедленный (в течение 2 суток) возврат к Конституции в редакции 2004 г., конституционную реформу и проведение президентских выборов не позднее декабря 2014 г.

В тот же день Янукович покинул Киев. На следующий день в телеэфир вышло видеоинтервью с ним, в котором он

[108] http://banderivets.org.ua/ 16.06.2014

заявил, что не намерен подавать в отставку и подписывать противозаконные решения Верховной рады, а события в стране квалифицировал как вандализм, бандитизм и госпереворот.

Верховная рада приняла постановление о том, что Янукович неконституционным образом самоустранился от осуществления полномочий и не выполняет своих обязанностей, а также назначила досрочные президентские выборы на 25 мая 2014 г. Обязанности президента Украины были возложены на председателя Верховной рады Александра Турчинова.

Новая власть получила признание со стороны ЕС и США, было сформировано временное правительство во главе с Яценюком.

Назначенный министр внутренних дел Аваков сообщил на своей странице в Facebook (имеет 178 450 подписчиков)[109] о возбуждении уголовного дела по факту массовых убийств мирных граждан, в связи с чем Янукович и ряд других должностных лиц объявлены в розыск[110].

27 февраля 2014 г. Янукович обратился к руководству России с просьбой обеспечить ему личную безопасность от экстремистов в связи с поступающими в его адрес угрозами. Он подчеркнул, что считает себя «действующим президентом» Украины, а решения Верховной рады последних дней, квалифицировал как нелегитимные, принимаемые в отсутствие многих парламентариев, причём многие из них подверглись физическому воздействию и покинули Украину.

Янукович также заявил о незаконности приказов, которые могут быть отданы на применение Вооружённых сил Украины внутри страны, ибо он не позволял армии этого. Янукович также обвинил оппозицию в невыполнении соглашения об урегулировании кризиса на Украине от 21 февраля.

---

[109] https://www.facebook.com/arsen.avakov.1 16.06.2014

[110] http://www.unian.net/politics/888892-yanukovich-obyyavlen-v-rozyisk-avakov.html 11.06.2014

После этого сообщения российские СМИ опубликовали заявление «источника во властных структурах РФ», утверждающего, что Янукович получит личную безопасность на территории России[111].

28 февраля 2014 г. Янукович на пресс-конференции в Ростове-на-Дону призвал российское руководство не оставаться безучастными к ситуации на Украине. По его словам, покинуть страну он оказался вынужден из-за непосредственной угрозы его жизни и жизням его близких[112].

Если в столице, в северных, центральных и западных регионах Украины новые власти, пользовались поддержкой населения, то на юго-востоке характер прихода к власти и потворство разгулу ультранационалистических организаций вызвали недовольство и волну протестов населения.

В Крыму была осуществлена смена исполнительных органов власти Севастополя и Автономной Республики Крым, а те, в свою очередь, отказались признать легитимность нового украинского руководства. В течение нескольких недель была провозглашена независимость Крыма, проведён общекрымский референдум.

17 марта 2014 г. на основании результатов референдума и Декларации о независимости, была провозглашена суверенная Республика Крым, в состав которой вошёл Севастополь в качестве города с особым статусом. На следующий день был подписан договор между Российской Федерацией и Республикой Крым о принятии Республики Крым в состав России, в соответствии с которым в составе России были образованы новые субъекты - Республика Крым и город федерального значения Севастополь[113].

---

[111] http://www.forbes.ru/news/251442-yanukovich-poprosil-rossiyu-obespechit-ego-bezopasnost 11.06.2014

[112] http://www.forbes.ru/news/251510-yanukovich-prizval-rossiyu-spasti-ukrainu-ot-khaosa 11.06.2014

[113] http://www.kremlin.ru/acts/20605 11.06.2014

5.1.2. Референдумы на востоке Украины

По примеру Крыма 11 мая 2014 г. на территории Луганской и Донецкой областей прошли референдумы о статусе региона. По итогам голосования, государственную самостоятельность региона и создание Луганской народной республики (ЛНР) поддержали 96,2% участников референдума, за независимость Донецкой народной республики (ДНР) проголосовали 89,7%.

Референдумы побудили Киев начать так называемую антитеррористическую, а по сути карательную операцию против республик с использованием авиации, бронетанковой техники и артиллерии, что привело к массовым жертвам и потокам беженцев, в т.ч. в Россию.

22 мая 2014 г. Верховный совет провозглашенной ДНР обратился к России с просьбой признать независимость ДНР, а 24 мая народный губернатор Донбасса Павел Губарев объявил, что провозглашенные ДНР и ЛНР объединились в составе единого государства Новороссия.

11 июня 2014 г. провозглашенная ЛНР обратилась к России и еще 14 государствам (Армении, Белоруссии, Казахстану, КНР, Сербии, Венесуэле, Кубе, Никарагуа и др.) с просьбой признать ее независимость.

Обе республики ведут работу по созданию совместной конституции, правительства и парламента, заявил депутат Верховной рады Украины, лидер движения «Юго-Восток» Олег Царев[114].

Кто и где воюет на Украине? Политический кризис на Украине привел к образованию многочисленных вооруженных формирований (рис. 5.1.)[115].

[114] http://www.km.ru/world/2014/06/12/protivostoyanie-na-ukraine-2013-14/742303-tsarev-obyavil-o-sozdanii-obshchego-parla 13.06.2014
[115] http://itar-tass.com/infographics/7793 14.06.2014

Киев	Хмельницкая	Черкасская	Херсонская	Одесская
Нацгвардия Украины	Нацгвардия Украины	Нацгвардия Украины	БТО* «Херсон» **230 чел.****	БТО «Шторм»
Николаевская	**Черниговская**	**Тернопольская**	**Кировоградская**	**Житомирская**
БТО «Святой Николай»	БТО «Чернигов» **200 чел.**	БТО «Тернополь» **430 чел.**	Нацгвардия Украины БТО «Кировоград» **128 чел.**	Нацгвардия Украины БТО «Полесье»
Сумская	**Львовская**	**Харьковская**	**Запорожская**	**Винницкая**
Нацгвардия Украины БТО «Сумы» **200 чел.**	Нацгвардия Украины БТО «Слобожанщина» БТО «Харьков» **до 900 чел.**	Нацгвардия Украины БТО «Слобожанщина» БТО «Харьков» **до 900 чел.**	Батальон МВД особого назначения «Азов» **150 чел.** БТО «Хортица»	Нацгвардия Украины Полк спецназначения Нацгвардии «Ягуар» БТО «Винница» **200 чел.**
Днепропетровская	**Киевская**	**Полтавская**	**Луганская** (Луганская народная республика)	
Нацгвардия Украины Батальон спецназа МВД «Днепр» **до 800 чел.** (финансируется губернатором И. Коломойским)	Нацгвардия Украины БТО «Киев-1» БТО «Киевщина» **142 чел.** БТО «Миротворец»	Нацгвардия Украины БТО «Каскад» БТО «Кременчуг» БТО «Полтава»	**САМООБОРОНА ЛНР** Армия Юго-Востока **3 тыс. - 4 тыс. чел.**, включая женский батальон **500 чел.**	**ПРАВИТЕЛЬСТВО УКРАИНЫ** Нацгвардия Украины Добровольческий БТО «Айдар»

Донецкая (Донецкая народная республика)

САМООБОРОНА ДНР
Народное ополчение Донбасса
от 800 до 2,5 тыс. чел., включая батальон «Восток»
100 чел.

7 ед. бронетехники, включая артустановку «Нона»
Народная армия Донецка
до 1 тыс. чел.
16 ед. бронетехники, включая артустановку «Нона», самолет Ан-2

ПРАВИТЕЛЬСТВО УКРАИНЫ
Нацгвардия Украины
25-й добровольческий батальон Нацгвардии Украины «Донбасс»
120 чел., большая часть - боевики «Правого сектора»

Добровольческий БТО «Украина» создан депутатом Верховной рады О. Ляшко
БТО «Артемьевск», «Донецк»

* БТО - Батальон территориальной обороны

** если численность не указана - данные засекречены

НАЦИОНАЛЬНАЯ ГВАРДИЯ УКРАИНЫ	БАТАЛЬОНЫ ТЕРРИТОРИАЛЬНОЙ ОБОРОНЫ
• создана в марте 2014 года • входит в систему МВД страны • присутствует в большинстве регионов • численность, по разным данным, от 15 тыс. до 60 тыс. чел. • имеет на вооружении около 100 ед. бронетехники, 20 транспортных самолетов и вертолетов	• начали формироваться в марте 2014 года • входят в систему МВД • должны быть созданы во всех 25 регионах. Пока существуют в 17 (включая батальон «Днепр») • общую численность планируется довести до 12 тыс. чел.

Источник: vv.gov.ua, mvs.gov.ua

ИТАР ТАСС

Рис. 5.1.

5.2. Зарубежные акторы кризиса на Украине

5.2.1. США – «системный интегратор» кризиса

Из попавшей в Интернет видеозаписи выступления помощника госсекретаря США В.Нуланд на заседании Фонда «США-Украина» в Вашингтоне в декабре 2013 г. стало известно, что США вложили 5 миллиардов долларов в демократизацию Украины.[116] В интервью CNN она подтвердила данный факт, поспешно добавив, что США не причастны к поддержке майдана.[117]

Нуланд явно лукавила. К началу марта 2014 г. она трижды за пять недель посещала Киев: нахваливала ассоциацию с ЕС и вела переговоры с оппозицией. В СМИ активно продвигались файлы о том, как она ходила по майдану и раздавала протестующим булочки, печенье и бутерброды.

При этом она была далеко не единственным американским политиком выразившим поддержку движению. Вместе с политиками США «Евромайдан» посещали высокопоставленные представители ЕС, ФРГ, Польши, Литвы, Швеции и т.д.

После разоблачений о финансировании США «Евромайдана» офис вице-президента США был вынужден опубликовать 7 июня 2014 г. факт-лист: Помощь США Украине.

В нем, в частности, говорится, что после обсуждений, состоявшихся между президентом Украины Порошенко и президентом Обамой 4 июня 2014 г. в Варшаве, вице-президент Байден объявил о дополнительной помощи украинскому правительству в размере 48 миллионов долларов. После консультаций с Конгрессом США эта помощь добавится к 1 миллиарду долларов гарантий по займам, подписанным 14 апреля 2014 г., 50 миллионам долларов пакета кризисного реагирования и 23 миллионам долларов помощи в вопросах

[116] https://www.youtube.com/watch?v=iNr3utHiwLA 16.06.2014
[117] http://www.rg.ru/printable/2014/04/22/demokratia-site-anons.html 14.06.2014

безопасности, о которой заявлено на данный момент. Если добавить к этому средства, выделенные ранее, получится, что США предоставляют свыше 184 миллионов долларов помощи Украине в этом году помимо гарантий по займам.

СБУ установило[118], что с первого дня «Евромайдана» каждый руководитель группы активного сопротивления получал денежное вознаграждение. За каждого активного бойца - по $200 в день и дополнительно - $500, если группа составляла более 10 лиц. Координаторы получали от $2000 за каждый день массовых беспорядков, при условии, что подконтрольная группа боевиков выполняет атакующие действия на правоохранителей.

СБУ также установило, что финансировались не только праворадикальные организации, но и оппозиционные партии. Средства поступали в посольство США в Киеве через дипломатический канал. В свою очередь посольство США переправляло деньги в центральные офисы ВО «Свобода» и ВО «Батьківщина». Сумма составляла порядка $20 млн в неделю. Далее эти средства распределялись на поддержку «Евромайдана» (функционирование системы жизнеобеспечения, взятки и подкуп отдельных чиновников, правоохранителей, оплата СМИ, расходы на агитацию и т.д.), а также ежедневные выплаты активным боевикам. В свою очередь, лидеры оппозиционных сил и радикальных группировок получали безналичные деньги на свои личные банковские счета.

По данным источника (Союз офицеров спецподразделений Украины), во время обыска, проведенного СБУ в помещениях центрального штаба «Батьківщини», из кабинета Александра Турчинова было изъято $17 млн. наличными. Кроме того, на изъятых сотрудниками СБУ серверах партии находилась информация относительно распределения средств на оплату жизнедеятельности майдана и проведение расчетов с боевиками радикальных группировок.

Также средства поступали и из стран Евросоюза.

---

[118] http://www.bolshoyvopros.ru/questions/826051-kto-finansiruet-pravyj-sektor-est-li-oficialnaja-informacija.html 17.06.2014

5.2.2. You Tube разоблачает политику США и их союзников

Сенсацией стал выложенный на You Tube телефонный разговор Нуланд с послом США в Киеве Д.Пайеттом (см. Приложение № 7)[119].

Анализ разговора показывает, что Нуланд умеет не только раздавать печенье. Так, Нуланд не устраивает, что европейцы, хотя и вмешиваются в дела независимой Украины, все же соблюдают некоторый декорум. Она женщина прямая, без политесов и загнала бы украинцев в НАТО.

Пойманная на матершине в адрес европейских союзников США, Нуланд извинилась за слова, но не за смысл.[120] Сейчас европейским лидерам труднее объясняться перед электоратом. В первую очередь, это касается ФРГ, которая больше всех вовлечена в дела Украины, в т.ч. и финансово.

Это усиливается тем, что сначала АНБ США прослушивает личные телефон немецкого канцлера, а теперь Нуланд посылает ту же Меркель... Однако ФРГ не обижается, ибо по сути оккупирована - там военные базы США, хотя Россия, главная победительница в войне, свои войска вывела двадцать пять лет назад. Теперь немцы понимают, что их руками США на Украине таскают каштаны из огня, и еще не ценят их стараний.

Нуланд не просто матерится. Она еще дает подробные инструкции: боксеру Кличко – не место в правительстве, а вот Яценюк – это человек, а когда сделка Янукович-оппозиция сложится, ее надо быстро провести через ООН. А ЕС пусть идет подальше….(мягкий перевод мата).

А теперь о личности Нуланд. Пикантность в том, что она дочь молдавских евреев, а по сути рулит известными своим антисемитизмом бандеровцами.

---

[119] http://russian.rt.com/article/21846 15.06.2014
[120] http://www.kp.ru/daily/26191/3079472/ 15.06.2014

Нуланд в 1991-1993 гг. служила в посольстве США в Москве, содействовала демократии огнем танков по парламенту, способствовала подъему экономики раздачей природных богатств и заводов друзьям Америки. На ее груди – медаль за Югославию (видимо за то, что удерживала Ельцина…). Служила она и в НАТО, продвигая его на Восток, способствовала нападению на Ирак и оккупации Афганистана.

Война и демократизация для нее семейный бизнес. Ее супруг – Роберт Каган, известный неоконсерватор - призывал к войне с Ираком, а затем с Ираном, а сама Виктория активно выступала за бомбовую демократизацию Сирии.

Парадоксально: в ходе только одной беседы Нуланд нанесла ущерб как союзу Вашингтона с Брюсселем и Берлином, так и проамериканским чувствам майдановцев. Она подставила и Керри – теперь ему сложнее обвинять Россию во вмешательстве.

Пытаясь оправдаться, Нуланд заявила на пресс-конференции в Киеве, что с 1991 года США потратили около $18 млрд. на Россию, а Украина за этот же период получила около $5 млрд. помощи.[121]

И здесь Нуланд лукавит, ибо ссумировала всю помощь России, в т.ч. на такие программы как «Глобальное партнерство», включая ликвидацию химоружия, утилизацию АПЛ, а также сферу нераспространения ядерного оружия и т.д.

5.2.3. Агентство США по международному развитию (USAID) как прикрытие для ЦРУ

Особая роль в «демократическом мессианстве» принадлежит Агентству США по международному развитию (АМР США) (United States Agency for International Development, USAID). Формально являясь независимым агентством, оно отвечает за невоенную помощь США более чем 100 странам

[121] http://news.liga.net/print/news/politics/2087552-ssha_vydelili_rossii_v_3_5_raza_bolshe_deneg_chem_ukraine_nuland.htm 14.06.2014

мира, в т.ч. и на Украине.[122] Однако руководитель Агентства и его заместитель назначаются президентом с согласия Сената и действуют в координации с госсекретарем США.[123]

USAID функционировало в России в 1992-2012 гг., выделив 2,7 млрд. долл. Агентство сотрудничало как с органами госвласти, так и с отдельными НПО, большинство из которых подпало под категорию «иностранных агентов».

В этом контексте следует подчеркнуть, что один из сотрудников USAID подтвердил в испанской газете «Rebelion» тот факт, что ЦРУ использует USAID в качестве прикрытия, в т.ч. для предоставления денежных средств и контрактов третьим сторонам, оказывающим содействие их операциям. Если раньше ЦРУ использовало USAID лишь в качестве вывески, то сегодня оно вовлечено против движений и государств, считающихся «враждебными» Вашингтону, что практически превращает USAID в военное ведомство.[124]

У экспертов не вызывает сомнения, что именно ЦРУ руководило операцией на Украине, как и в Югославии, Сирии, Ираке и др.[125] Это подтверждается признанным Белым домом фактом, что директор ЦРУ Бреннан под чужой фамилией 12 апреля 2014 г. совершил поездку в Киев, после которой началась антитеррористическая операция силовиков. На проведение подобных операций ЦРУ выделяет примерно 7,5 миллиарда долларов. Ситуация с Крымом, который отошел к России, и угроза гражданской войны на юго-востоке - прямое следствие личной ошибки Бреннана при анализе ситуации. Именно поэтому и потребовался его визит в Киев. Не надо забывать и того, что последний этаж в здании СБУ занимают инструкторы ЦРУ, куда запрещен доступ украинским офицерам.[126]

---

[122] http://ukraine.usembassy.gov/usaid.html 16.06.2014

[123] http://ru.wikipedia.org/wiki/%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D1%81%D1%82%D0%B2%D0%BE_%D0%A1%D0%A8%D0%90_%D0%BF%D0%BE_%D0%BC%D0%B5%D0%B6%D0%B4%D1%83%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%BE%D0%BC%D1%83_%D1%80%D0%B0%D0%B7%D0%B2%D0%B8%D1%82%D0%B8%D1%8E 15.06.2014

[124] http://www.inosmi.ru/usa/20091216/157038361.html#ixzz25Ud375Pe 15.06.2014

[125] http://lenta.ru/news/2014/05/11/brennan 15.06.2014

[126] http://lifenews.ru/news/131365 15.06.2014

5.2.4. Троллинг по лекалам Госдепа США и USAID

В 2006 г. в Госдепе появилась группа специалистов (Digital Outreach Team) для анализа сообщений и дискуссий в международных и национальных соцсетях[127] в особенности там, где сильны антиамериканские настроения. Кроме этого, члены Digital Outreach Team принимают участие в дискуссиях, регистрируясь в соцсетях в качестве участников или модераторов с целью разъяснения позиции США на международной арене и ликвидации дезинформации со стороны противников США. В зависимости от поставленных задач и целевой аудитории сотрудники имеют возможность самостоятельно выбирать стиль и содержание публикуемых сообщений, используя в т.ч. троллинг.

Следует заметить, что в 2007–2008 гг. были созданы еще пятнадцать подобных отделов в USAID и разведсообществе США[128].

Для более эффективной работы этих отделов разработаны инструкции. Характерно, что в сети появился её украинский аналог[129]. Приведем наиболее яркие советы:

- Не ведитесь на провокации, не отвечайте агрессией на агрессию.
- Атака на пост, видео, комментарий проводится целенаправленно, группами по 10-20 человек, в одиночку вас просто разгромят фактами.
- Вынуждайте оппонента любыми действиями применить мат и прочие нецензурные выражения.
- Постоянно указывайте оппоненту, что он ведет себя некультурно.

[127] Digital Outreach Team (www.state.gov/iip/programs/)
[128] U.S. Public Diplomacy Actions Needed to Improve Strategic Use and Coordination of Research. GAO Report. 2007. P. 31.
[129] http://oper.ru/news/read.php?t=1051613356

- Если оппонент задавил вашу ложь фактами, делайте упор на его грамматические ошибки, это деморализует его, вуалируя вашу ложь.
- Пытайтесь внести раскол между оппонентами, например, люди встают на защиту Донецка, а Вы напишите, что сами из Донецка и смысла нет бороться, только хуже будет.
- Не используйте слова: захват власти, бандеры, боевики, террористы, нацисты, националисты. Всегда говорите - народ Украины.
- Не пишите, что мы за Европу, пишите, что мы за единую Украину.
- Постарайтесь писать по-русски, украинская речь многих отталкивает.
- Пытайтесь убедить оппонентов, что их обманули или обманывают.
- Пытайтесь убедить, что России от Украины нужны только ресурсы и рабочая сила.
- Пытайтесь убедить, что в России всё плохо, используйте фото глубинок, старых зданий, свалок; идеальны демотиваторы про старушек, пенсию, голодных детей и иные факты человеческой жалости.
- Показывать по максимуму как жили Янукович и депутаты ПР, делать акцент на то, что это всё разворованные народные, ваши деньги.
- Доказывать, что Украина будет сильной только вместе, запугивать, что Россия сделает своими рабами Юго-Восток и Крым.
- Если оппонент будет вам показывать успехи России - упрекать его, что он подвергся кремлевской пропаганде. Убедить его, что у вас якобы родные в России, которые в ужасе от нищеты.
- Точно так же поступать, только наоборот, если оппонент будет показывать факты нищеты и разрухи в Европе или США.

- Если оппонент доказал, что Нацбанк контролируется США, делайте акцент, что так во всех странах для удобства экономик. Акцентируйте: США и ЕС хотят помочь Украине и очень за неё переживают.

5.2.4.1. Примеры зарубежного участия в информационной войне в Крыму

На многих форумах по умолчанию определяется IP адрес. На одном из таких ресурсов в Крыму[130] «Гость» якобы из СНГ вбрасывает тему отстранения чиновников за отказ снятия флагов другого государства (РФ) со здания Верховного Совета Крыма (рис. 5.2.).

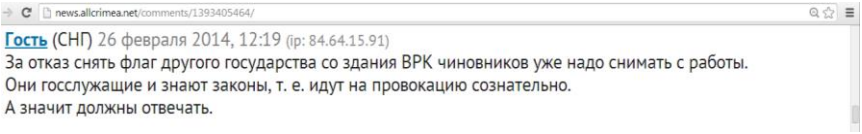


Рис. 5.2.

Проверяем откуда человек выходил в интернет по его IP адресу здесь: **http://ip-whois.net/ip_geo.phpA** вставляем его IP:84.64.15.91 и видим, что **«Гость» из СНГ на самом деле из UK** (рис. 5.3.)**!!!**

Рис. 5.3.

[130] http://news.allcrimea.net/comments/1393405464/

А вот и его точная геолокация на карте со спутника (рис. 5.4.)!

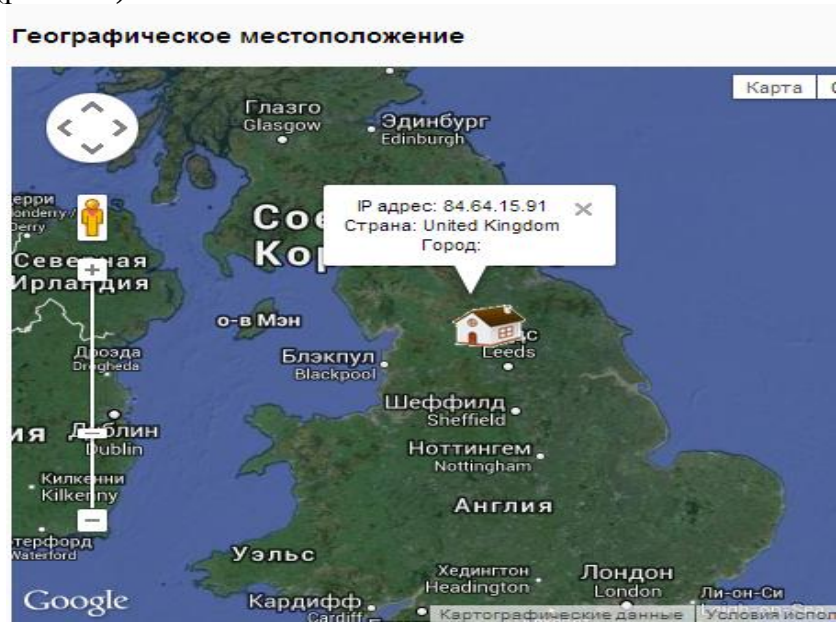


Рис. 5.4.

А теперь посмотрим, как ведут себя другие «земляки» на этом форуме. Так, пользователь из Ванкувера выбрал себе ник «украина» и пишет, что Крым – это Украина (рис. 5.5.):
IP адрес: 67.168.213.170
Страна: United States
Регион: Washington
Город: Vancouver

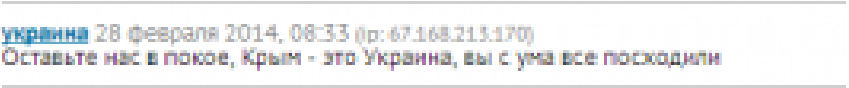


Рис. 5.5.

Человек из Люксембурга указал город «Ялта» и троллит Януковича (рис. 5.6.).

IP адрес: 94.242.252.41
Страна: Luxembourg
Регион: Luxembourg
Город: Steinsel

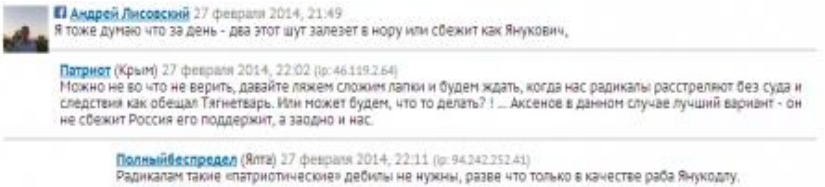


Рис. 5.6.

5.2.5. Тайны «Евромайдана»: виртуальные файлы свидетельствуют

5.2.5.1. «Дело снайперов»

Сенсационной оказалась запись разговора Верховного представителя ЕС по иностранным делам Кэтрин Эштон и главы МИД Эстонии Урмаса Паэта, которая, как следует из описания, попала в распоряжение работников Службы безопасности Украины.[131]

Оба европейских политика в ходе разговора обсуждают свои впечатления о ситуации на Украине. Во время беседы Урмас Паэт также упоминает о том, что снайперы, стрелявшие в людей в Киеве, были наняты лидерами Майдана.

В беседе Паэт рассказывает, что все улики, которые ему показывали, свидетельствуют, что и протестующих, и сотрудников правоохранительных органов убивали одни и те же снайперы. «Очень тревожит, что новая коалиция не хочет расследовать эти события, и теперь становится всё яснее, что за этими снайперами стоял не Янукович, а кто-то из новой коалиции», - рассказал он. Паэт опасается, что если «эта ис-

[131] http://russian.rt.com/article/23679#ixzz34SIQF 11.06.2014

тория начнёт жить своей жизнью, то сразу дискредитирует новую коалицию».[132]

Следует подчеркнуть, что в настоящее время «дело снайперов» как и расследование событий в Одессе зашли в тупик…

5.2.5.2. Анализ перехваченной переписки военного атташе США с офицером Генштаба ВС Украины

Группа Anonymous Ukraine взломала почту помощника американского военного атташе в Украине Джейсона Греша (Jason Gresh) и представителя Генштаба ВС Украины Игоря Процика (Igor Protsyk). Письма подлинные, т.к. прошли проверку на валидность (DKIM на месте, все верифицируется).[133]

Из писем следует, что авторы разрабатывали сценарии для дестабилизации Крыма. Так, Греш обращается к Процику с просьбой разработать план для нарушения работы транспортных узлов на юго-востоке Украины для того, чтобы дискредитировать вооруженные силы России. В свою очередь, Процик контактирует с боевиком «Правого сектора» Василем Лабайчуком для того, чтобы тот организовал нападение на авиабазу 25 авиационной бригады украинских военно-воздушных сил в Мелитополе.

Наиболее интересные фрагменты переписки (перевод).[134]

From: «Gresh, Jason P»
To: igor.protsyk@gmail.com, i.v.protsyk@mil.gov.ua
Subj: Peninsula
Date: Sun, 9 Mar 2014 17:57:09 +0200

[132] МИД Эстонии подтвердил подлинность разговора
[133] http://slivmail.com/gresh 17.06.2014
[134] http://slivmail.com/gresh 16.06.2014

Игорь,

События быстро развиваются в Крыму. Наши друзья в Вашингтоне ожидают более решительных действий от сети.

Я думаю, пришло время для реализации плана, который мы обсуждали в последнее время. Ваша задача, чтобы вызвать некоторые проблемы транспортных узлов на юго-востоке, чтобы подставить соседа.Это создаст благоприятные условия для Пентагона и Компании, чтобы начать действовать.

Не тратьте время, мой друг.

С уважением

JP

From: Igor Protsyk
To: krivonis.te@gmail.com
Subj: Активні дії у Мелітополі
Date: Tue, 11 Mar 2014 05:50:35 -0700

Василь, нужно очень быстро провести активные действия в Мелитополе. Там 25 авиатранспортная бригада. Надо замарать наших заклятых друзей и хороших соседей. Думаю, что ты понял меня.

Только действуйте внимательно и осторожно. 25 бригада сейчас на боевых заданиях, так что не делаете самолетам большой вред. Там есть уже поврежденные самолеты, вот с ним можно делать все. Их бортовые номера вам дадут. Помни, надо, чтобы все было как настоящая атака российского спецназа.

Комбриг там умный человек. Подробностей он не будет знать, но в крайнем случае к нему можно обратиться. Мы его предупредим.

From: Василь Лабайчук
To: kolyarny@gmail.com
CC: igor.protsyk@gmail.com
Subj: Потрібно терміново пошуміти
Date: Tue, 11 Mar 2014 09:20:46 -0700

Олег, нужно срочно пошуметь от имени москалей на аэродроме в Мелитополе. Это надо сделать до 15 марта. Сам понимаешь почему.

Прежде всего тебе надо связаться с Пашкой Тарасенко. Ты его должен знать, он из местной Свободы и владеет темой. К тебе приедут 10-12 ребят из Центра. Лучшие бойцы Тризуба. Главным там Миша, ты его тоже должен знать. Подробности узнаешь у него. Надо людей встретить и обеспечить всем необходимым.

Действуйте осторожно. Разговаривать только на русском языке. 25 бригада сейчас выполняет боевые задачи, поэтому не делайте большой вред самолетам. Там есть много металлолома, с ним можно делать все. Поврежденные самолеты вам укажут . Необходимо, чтобы все было как настоящая атака соседского спецназа. Но без трупов. Дай мне еще раз твой счет. Деньги придут вовремя, не волнуйся.

Смотри приложение. Это пример действий. Решение принимай лично.

Приложение к письму (рис. 5.7.):

Рис. 5.7.

Письмо начальника Генштаба ВС Украины главнокомандующему объединенных вооруженных сил НАТО в Европе[135]

От: oleksiy.nozdrachov@ukr.net
Кому: protsyk@ukr.net
Тема: (Нет темы)
Дата: 11.03.2014 06:55

Best regards
Nozdrachov Oleksiy
COL, Ukrainian General Staff,
Main Directorate of Military Cooperation & PKO,
Deputy, Western Europe & North Americabranch

К письму приложен файл письма начальника Генштаба ВС Украины к командующему НАТО в Европе. Ниже перевод этого письма:

[135] http://nstarikov.ru/club/37329?print=print 17.06.2014

Уважаемый господин генерал!

Рад заметить, наши телефонные разговоры происходят на постоянной основе.

Учитывая тяжелые времена, для Вооруженных Сил Украины очень важна поддержка всех стран-партнеров, особенно Соединенных Штатов.

I. Ситуация в Украине

В начале хочу остановиться на ситуации в Украине.

К сожалению, продолжается эскалация кризисной ситуации в Юго-Восточных регионах Украины и Автономной Республике Крым. Российская Федерация активно наращивает военное присутствие в Крыму. В настоящее время продолжается захват подразделений Воздушных и Военно-Морских Сил ВС Украины в Крыму. Вооруженные Силы Украины начали широкомасштабные тактические учения по всей территории Украины. Основной целью является завершение боевого слаживания подразделений и органов военного управления.

II. Перспективы военного сотрудничества

Хочу поблагодарить за помощь, которая предоставляется аппаратом военных атташе при Посольстве США в Украине.

Мы проработали перечень военной помощи, которая нужна Вооруженным Силам Украины в первую очередь, и я знаю, что первый самолет Воздушных Сил США прибывает в ближайшее время. Нами уже организуется работа по обеспечению бесперебойного получения имущества. Помощь, получаемая от США будет широко освещена в украинских и мировых средствах массовой информации. Я уверен, что мы оба понимаем важность получения этой помощи в кратчайшие сроки.

В завершение

Все же надеюсь, что Вы найдете возможность осуществить кратковременный визит в Украину и лично ознакомиться с ситуацией на месте.

Благодарю Вас за плодотворную и конструктивную беседу и надеюсь на дальнейшее взаимовыгодное сотрудничество.

5.3. «КиберБеркут» vs «Киберсотня»

3 марта 2014 г. в виртуальном фронте Украины появился «КиберБеркут» - группа хактивистов после расформирования спецподразделений милиции «Беркут». Состав сообщества неизвестен, его члены соблюдают анонимность. «КиберБеркут» позиционирует себя как хакерская группировка, которая «помогает Украине сохранить независимость от военной агрессии Запада, готового защитить правительство неофашистов».

В первом сообщении говорится, что «как несгибаемый «Беркут» стоял до конца, так и «КиберБеркут» будет охотиться на фашистскую нечисть, пока не истребит её! Сегодня мы начали взлом сайтов, чтобы заткнуть поток лжи запуганных СМИ! Мы заявляем, что отстоим Украину, сбережем её историю и защитим будущее её народа!!!»[136]

Среди многочисленных атак, взломов и иных действий «КиберБеркута» заслуживают внимания следующие:

- DDoS атаки на продавшиеся радикалам СМИ: за первые 10 дней – были блокированы десятки сайтов;
- 15 марта 2014 г. атака на ресурсы НАТО:

http://ccdcoe.org
http://nato.int
http://nato-pa.int.

http://ccdcoe.org - это сайт Таллиннского киберцентра НАТО (NATO Cooperative Cyber Defence Centre of Excellence). Дело в том, что по просьбе новых властей на Украину прибыла группа сотрудников киберцентра и назвала себя майдановской «Киберсотней». Прикрываясь ими, Запад ведет

[136] http://cyber-berkut.org/

активную пропаганду среди населения через СМИ и социальные сети, блокирует объективные источники информации, скрывает действия преступников, называющих себя «законной властью». При этом в Киев прибыл весь цвет киберруководства НАТО во главе с полковником А.Сузиком. В целях подрыва доверия к «КиберБеркуту» эта группа создавала его ложные аккаунты в соцсетях (рис. 5.8.).

Рис. 5.8.

- 22.03.2014 взломана переписка политиков, в т.ч. украинских НПО с посольством США и американскими фондами (рис. 5.9.).

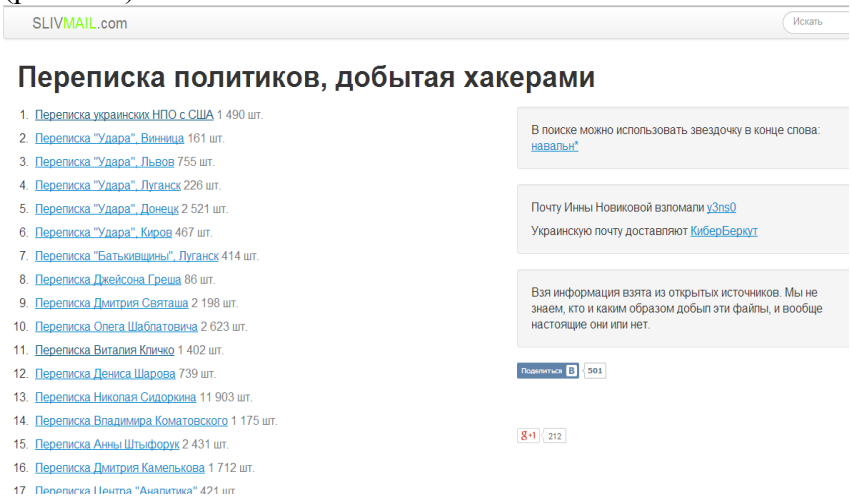
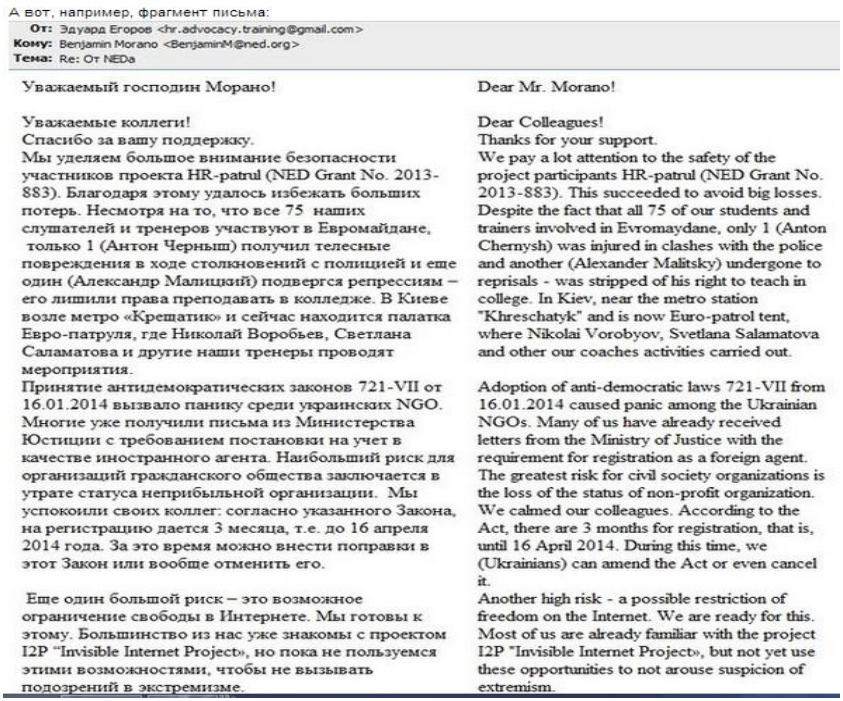


Рис. 5.9.

Небезынтересна переписка Э.Егорова – руководителя НПО «Учебно-методический центр защиты прав человека», который активно участвовал в протестах на Украине (рис. 5.10.). Из переписки видно, что за финансирование деятельности в Украине отвечал Национальный фонд поддержки демократии, который получает деньги от Конгресса США и продвигает «американскую демократию» по всему миру. А за координацию усилий на Майдане, как оказалось, отвечает отдел прессы, образования и культуры посольства США!



А вот, например, фрагмент письма:

От: Эдуард Еропов <hr.advocacy.training@gmail.com>
Кому: Benjamin Morano <BenjaminM@ned.org>
Тема: Re: От NEDa

Уважаемый господин Морано!

Уважаемые коллеги!
Спасибо за вашу поддержку.
Мы уделяем большое внимание безопасности участников проекта HR-patrul (NED Grant No. 2013-883). Благодаря этому удалось избежать больших потерь. Несмотря на то, что все 75 наших слушателей и тренеров участвуют в Евромайдане, только 1 (Антон Черныш) получил телесные повреждения в ходе столкновений с полицией и еще один (Александр Малицкий) подвергся репрессиям – его лишили права преподавать в колледже. В Киеве возле метро «Крещатик» и сейчас находится палатка Евро-патруля, где Николай Воробьев, Светлана Саламатова и другие наши тренеры проводят мероприятия.
Принятие антидемократических законов 721-VII от 16.01.2014 вызвало панику среди украинских NGO. Многие уже получили письма из Министерства Юстиции с требованием постановки на учет в качестве иностранного агента. Наибольший риск для организаций гражданского общества заключается в утрате статуса неприбыльной организации. Мы успокоили своих коллег: согласно указанного Закона, на регистрацию дается 3 месяца, т.е. до 16 апреля 2014 года. За это время можно внести поправки в этот Закон или вообще отменить его.

Еще один большой риск – это возможное ограничение свободы в Интернете. Мы готовы к этому. Большинство из нас уже знакомы с проектом I2P "Invisible Internet Project», но пока не пользуемся этими возможностями, чтобы не вызывать подозрений в экстремизме.

Dear Mr. Morano!

Dear Colleagues!
Thanks for your support.
We pay a lot attention to the safety of the project participants HR-patrul (NED Grant No. 2013-883). This succeeded to avoid big losses. Despite the fact that all 75 of our students and trainers involved in Evromaydane, only 1 (Anton Chernysh) was injured in clashes with the police and another (Alexander Malitsky) undergone to reprisals - was stripped of his right to teach in college. In Kiev, near the metro station "Khreschatyk" and is now Euro-patrol tent, where Nikolai Vorobyov, Svetlana Salamatova and other our coaches activities carried out.

Adoption of anti-democratic laws 721-VII from 16.01.2014 caused panic among the Ukrainian NGOs. Many of us have already received letters from the Ministry of Justice with the requirement for registration as a foreign agent. The greatest risk for civil society organizations is the loss of the status of non-profit organization. We calmed our colleagues. According to the Act, there are 3 months for registration, that is, until 16 April 2014. During this time, we (Ukrainians) can amend the Act or even cancel it.
Another high risk - a possible restriction of freedom on the Internet. We are ready for this. Most of us are already familiar with the project I2P "Invisible Internet Project», but not yet use these opportunities to not arouse suspicion of extremism.

Рис. 5.10.

- 24.03.2014 перехвачен и выложен в сеть телефонный разговор от 18 марта 2014 г. бывшего заместителя секретаря Совета нацбезопасности и обороны Украины Н.Шуфрича и бывшего премьер-министра Ю.Тимошенко. Обсуждалась возможность силового столкновения с Россией.
- Тимошенко говорила Шуфричу, что оставит от России «выжженное место», уничтожит восемь миллионов русских, проживающих на Украине, и готова сама взять автомат и «стрелять кацапов».
- Разговор в Интернет, похоже, выложили с помощью сотрудников СБУ. Из записи удалены фрагменты, которые могут скомпрометировать третьих лиц.
- 9.04.2014 «КиберБеркут» наносит ответный удар по американским частным военным компаниям, которые проли-

ли кровь жителей в так называемой АТО на юго-востоке Украины. Дефейс[137] компаний Triple Canopy и Tidewater Global Services, а также DDoS-атака на Greystone Limited и Academi – бывшую ЧВК Blackwater.

- 22.04.2014 «КиберБеркут» вскрыл переписку Авакова и его бывшего пресс-секретаря и делового партнера Дмитрия Брука.

В переписке недвусмысленно указывается, что убийство Сашко Билого было спланировано Аваковым, а в качестве «расплаты» за его смерть так называемое правительство выдает Ярошу бойцов «Беркута».

Кроме того, из переписки видно, как цинично власть устраняет неугодных им журналистов, например К.Долгова.

- 29.04.2014 г. «КиберБеркут» благодаря стараниям группировки Anonymous Ukraine выложил архив переписки (около 2 тыс. писем) (рис. 5.11).

[137] Deface - тип хакерской атаки, при которой главная страница веб-сайта заменяется на другую, как правило, вызывающего вида. Зачастую доступ ко всему остальному сайту блокируется, или же прежнее содержимое сайта вовсе удаляется

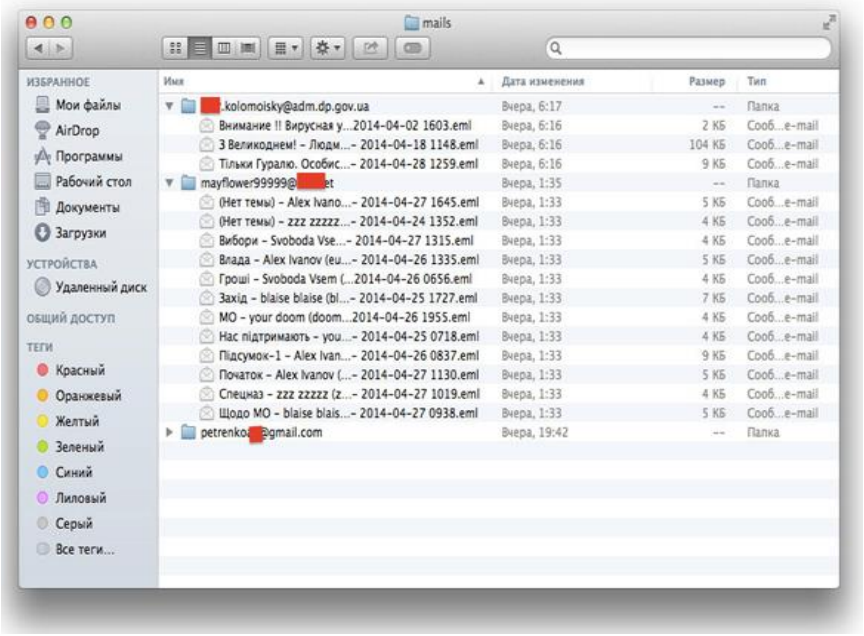


Рис. 5.11.

- Анализ лишь одного из мэйлов, который был отправлен главой Днепропетровской области, олигархом Коломойским львовскому прокурору Владимиру Гуралю с пометкой «Секретно», - сенсация. На Украине, якобы, готовится военный переворот: планируется свергнуть председателя Верховной Рады, и.о. президента Украины Александра Турчинова, а «затевается это все под Тягнибока и его «Свободу».
- Коломойский рекомендует устроить неофициальную проверку данных «о готовящемся заговоре во главе с адмиралом Тенюхом». Он назвал и других «путчистов», в т.ч. и генерала Петренко – представителя Украины в НАТО, в переписке которого, были найдены доказательства готовящегося заговора.
- 03.05.2014 КиберТрибунал вынес приговор виновницам в сожжении живых людей в Одессе.

- 14.05.2014 КиберАрмия наносит удар по виновникам Одесской трагедии.
- 15.05.2014 Антифашистское движение в киберпространстве набирает силы.
- 23.05.2014 электронная система ЦИК Украины уничтожена за три дня до президентских выборов.
- 25.05.2014 заблокированы телефоны избиркомов.
- 25.05.2014 уничтожена компьютерная сеть администрации Днепропетровской области, ЦИК продолжает лгать.
- 04.06.2014 из обращения «КиберБеркута»:

«Киевская хунта продолжает геноцид украинского народа. Ежедневно на юго-востоке нашей страны от авиационных и артиллерийских обстрелов гибнут десятки мирных людей. Сотни стариков и детей лишились своих домов, разрушены школы, больницы и детские сады. Редакторы и журналисты подконтрольных Киеву СМИ, находясь в страхе за свою жизнь, вынуждены замалчивать «кровавую» правду про события на юго-востоке.

Мы, «КиберБеркут», открываем раздел на нашем сайте, посвященный преступлениям хунты против украинского народа. Мы будем собирать присланные Вами документальные свидетельства преступлений против мирного населения (видеосъемки бомбардировок жилых районов, больниц, школ, детских садов, бортовые номера техники украинской армии, совершающей обстрелы и т.п.). Виновные предстанут перед «Народным Трибуналом»!

Мы обращаемся к украинским военнослужащим.

Солдаты и офицеры ВС Украины!

Сегодня мы, «КиберБеркут», обращаемся к Вам с призывом остановиться. Киевская власть под предлогом проведения АТО втянула Вас в кровавую бойню. Вас обманули. Вас сделали соучастниками военных преступлений, совершаемых «Правым сектором» и Национальной гвардией, которые за деньги олигархов готовы на все. Не уподобляйтесь этим наемникам. В Ваших силах не допустить убийство украин-

ских женщин и детей, которые никогда не были террористами!

Вскоре кто-то обязательно ответит за совершенные преступления против мирного населения юго-востока, и мы не исключаем, что киевская хунта всю ответственность возложит на простых офицеров. Помните об этом.»

5.4. «Виртуальное» ополчение

Пользуясь отсутствием единой авторитетной информационной площадки, в социальных сетях, якобы от имени ополчения Юго-Востока, всё чаще появляются как отдельные вбросы дезинформации, так и целые сообщества, которые умело и дозировано подмешивают ложь.

По данным ополченцев, в этих спецмероприятиях активно задействованы силы и средства СБУ и АНБ США.

В целях продвижения достоверной и оперативной информации об истинном положении дел на Юго-Востоке ополчение создало свой сайт (рис. 5.12.).[138]

Кроме того, созданы аккаунты в сетях в Facebook[139], Vkontakte[140], а также видеоканал на Youtube[141].

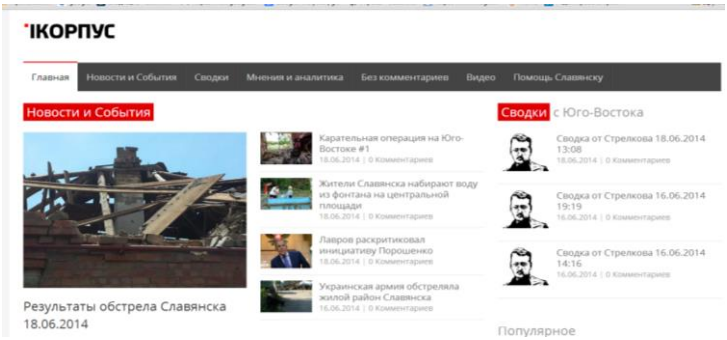


Рис. 5.12.

[138] http://icorpus.ru/ 19.06.2014
[139] https://www.facebook.com/infokorpus 19.06.2014
[140] http://vk.com/icorpus 19.06.2014
[141] http://www.youtube.com/channel/UCUKBgsn2phUucpQGZA-K_Vw 19.06.2014

Как и непрерывные обстрелы мирных граждан и гражданских объектов на Юго-Востоке Украины, сайт ополченцев также сразу после его открытия попал под массированную кибератаку (рис. 5.13.).[142]

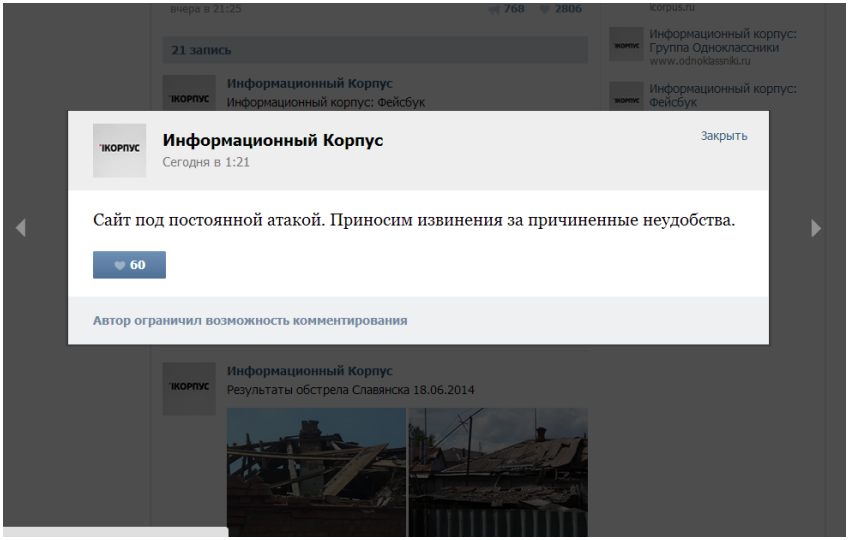


Рис. 5.13.

Власти Киева всеми способами пытаются задушить правду. Для этого они готовы пойти на всё: от виртуального убийства противника до реального убийства журналистов, несущих миру правду об их злодеяниях.

[142] http://vk.com/icorpus?w=wall-72627612_98 19.06.2014

«Я понял, что я - часть того,
что приносит намного больше вреда, чем пользы»

Э.Сноуден

Все тайное рано или поздно становится явным.

Сократ

6. «SNOWDENGATE»: ТОТАЛЬНЫЙ КОНТРОЛЬ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА СПЕЦСЛУЖБАМИ США И ИХ СОЮЗНИКОВ

Разоблачения Э.Сноудена вызвали острую полемику как в США, так и в мире о допустимости массового негласного наблюдения и балансе между защитой персональных данных и обеспечением национальной безопасности в эпоху после терактов 11 сентября 2001 г.

Действительно, обнародованные в ряде СМИ экс-сотрудником ЦРУ и Агентства национальной безопасности (АНБ) США[143] Эдвардом Сноуденом секретные документы американских спецслужб разоблачают многочисленные факты

[143] Разведывательное сообщество США (United States Intelligence Community, IC) - собирательный термин для обозначения 16-и отдельных правительственных учреждений. Общее руководство с 2005 г. осуществляет директор Национальной разведки. С образованием министерства внутренней безопасности и отделением ЦРУ от руководства разведсообщества данные всех разведсообществ аккумулирует директор Национальной разведки, а ЦРУ работает с так называемой human intelligence - агентурой. Это совпало с общим трендом последнего времени, когда все большую роль играет SIGINT - signal intelligence, то есть массив электронной информации. Кроме того, за последние 15–20 лет за счет спутников и других средств мощное развитие получила геопространственная разведка. АНБ (National Security Agency/Central Security Service, NSA/CSS) отвечает за сбор и анализ зарубежных трафиков, их координат, направлений, криптоанализ, а также за защиту государственных коммуникационных каналов от действий аналогичных служб других государств http://ru.wikipedia.org/wiki/ 17.12.2013

незаконной деятельности[144] США и их союзников в глобальном информационном пространстве.

Анализ публикаций показывает, что США, грубо попирая права граждан, создали глобальную систему электронного шпионажа, перехвата и обработки личных данных пользователей разных стран мира: телефонных разговоров, смс-сообщений, переписки в социальных сетях и по электронной почте.

АНБ взламывало операционные системы смартфонов практически всех ведущих производителей: «iPhone» компании «Apple», «BlackBerry», «Android», перехватывая личные данные пользователей.

В 2010-2011 гг. спецслужбы разработали программу по сбору геолокационных сведений об абонентах сотовых сетей. Так, АНБ ежедневно собирает и сохраняет около пяти миллиардов записей о местонахождении и передвижениях владельцев мобильных телефонов по всему миру, а затем при помощи специальной программы CO-TRAVELER проводит контент-, ивент- и коннект-анализ, а также мониторинг передвижения людей.

С 2010 г. АНБ обрабатывает информацию о социальных контактах граждан США, их персональных данных, в том числе телефонных звонках, Интернет-активности, банковских кодах, страховых сведениях, регистрационных списках избирателей.

---

[144] Программы АНБ США по сбору данных о телефонных переговорах американцев противоречат конституционным нормам. Таково предварительное определение, вынесенное 16.12.2013 в Вашингтоне федеральным окружным судьей Ричардом Леоном. Ранее АНБ на основании судебного решения от 1979 г. оправдывалось, что метаданные о звонках не подпадают под действие четвертой поправки, однако судья счел, что «спустя 34 года использование телефонов вышло на совсем другой уровень, и сегодня подобная информация по мере накопления позволяет выстраивать подробную картину о личной жизни каждого». Скандалы вокруг разоблачений в отношении АНБ привели к отставке его главы. В октябре 2013 г. комитет по разведке сената США одобрил законопроект, накладывающий ограничения на деятельность АНБ. Будут ограничены возможность для массового сбора телефонных и электронных данных, сроки их хранения, введена уголовная ответственность за умышленный несанкционированный доступ к подобным сведениям. Администрация Б.Обамы изучает возможность внесения серьезных корректив в работу спецслужб.
http://www.rg.ru/2013/12/17/sud-site.html 17.12.2013

АНБ способно хранить собранные данные о жителях США вплоть до 5 лет без получения специального разрешения. Единственным формальным ограничением является то, что собранная информация должна способствовать предотвращению угроз национальной безопасности или проведению расследований. Она может быть передана союзным государствам или иностранным организациям, при условии сохранения анонимности пользователей.

В рамках проекта «Boundless Informant» АНБ только в марте 2013 г. собрало около 97 млрд. файлов информации о звонках иностранных граждан по всему миру[145], в том числе об Иране (14 млрд. файлов), Пакистане (13,5 млрд.), Иордании (12,7 млрд.), Египте (7,6 млрд.), Индии (6,3 млрд.).

6.1. Вторая молодость «Эшелона»

АНБ тесно взаимодействует с иностранными разведками. США, Великобритания, Канада, Австралия и Новая Зеландия входят в секретное союзное объединение по сбору данных в рамках глобальной системы радиоэлектронной разведки «Эшелон» (AUSCANNZUKUS или Five Eyes), основанной в формате США-Великобритания ещё в 1947 г. Спецслужбы этих стран обмениваются развединформацией, в том числе о гражданах своих государств. Позднее к альянсу присоединился ряд стран НАТО, в том числе Норвегия, Дания, ФРГ и Турция.[146]

Схема системы «Эшелон» - спутники связи, наземные станции, подключение к кабелям связи (рис. 6.1.).[147]

[145] The Guardian от 11 июня 2013 г.
[146] http://ru.wikipedia.org/wiki/%D0%AD%D1%88%D0%B5%D0%BB%D0%BE%D0%BD_%28%D1%81%D0%B5%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D0%B0%D1%8F_%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D0%B0%29 17.12.2013
[147] http://www.3dnews.ru/578591/ 21.06.2014

Рис. 6.1.

В рамках проекта «Prism» АНБ и британский Центр правительственной связи - ЦПС (Government Communications Headquarters, GCHQ)[148], начиная с 2007 г., наладили сотрудничество с мировыми ИКТ-компаниями: «Microsoft», «Yahoo», «Google», «Facebook», «PalTalk», «AOL», «Skype», «YouTube» и «Apple» для сбора и обмена разведданными (рис. 6.2.).[149]

[148] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data 20.06.2014
[149] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data 20.06.2014

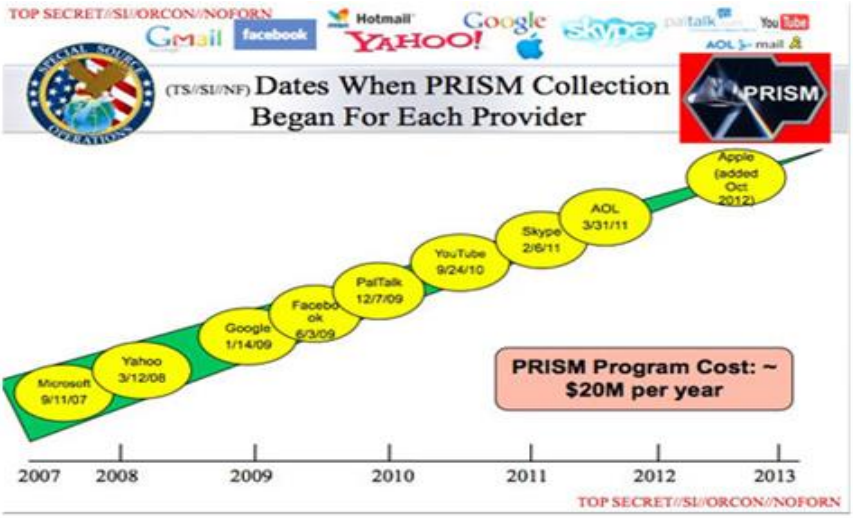


Рис. 6.2.

Такое сотрудничество позволяет спецслужбам прочитывать Интернет-историю, электронные письма пользователей и отслеживать передачу файлов в глобальном информационном пространстве.

6.2. «Под колпаком» лидеры государств и иностранные дипломаты

АНБ прослушивало телефонные разговоры 35 глав различных государств. Контактные данные агентство получало от сотрудников различных ведомств, в том числе Белого дома, Госдепа и Пентагона[150].

Спецслужбы США отслеживали переговоры канцлера Германии А.Меркель с 2002 г, в том числе и до ее избрания на

[150] The Guardian от 24 октября 2013 г.

этот пост[151], разговоры членов правительства Испании[152] и перехватывало Интернет-трафик и телефонные переговоры президента Бразилии Дилмы Роуссефф и мексиканского лидера Энрике Пенья Ньето. Электронную почту последнего спецслужбы США начали вскрывать еще за месяц до его избрания на пост президента[153]. В 2010 г. АНБ получило доступ к электронной почте президента Мексики Фелипе Кальдерона и письмам мексиканских министров, которые касались дипломатических, экономических и политических вопросов[154].

Британский ЦПС прослушивал телефонные разговоры и мониторил компьютеры министра финансов Турции и 15 членов турецкой делегации, а также других участников саммита «Группы двадцати» в Лондоне в 2009 г., в том числе Президента России Д.А.Медведева[155]. В 2005 г. британский ЦПС следил за деятельностью министра иностранных дел ЮАР и другими дипломатами[156].

Характерно, что **спецслужбы США и Великобритании незаконно взламывали практически все используемые в сети Интернет стандарты криптографии.** В силу этого они имели доступ к чувствительной информации, содержащей, в том числе и коммерческую тайну компаний по всему миру, и иным зашифрованным данным.

Для взлома шифров АНБ использует имеющиеся у него суперкомпьютеры, а также прибегает к услугам высокопрофессиональных хакеров. Ежегодно на эти цели США тратят более 250 млн. долларов[157].

При этом АНБ предпринимает попытки взлома так называемого «Лукового маршрутизатора», разработанного в США и позволяющего пользователям сохранять анонимность в сети

[151] Der Spiegel от 26 октября 2013 г.
[152] El Pais от 25 октября 2013 г.
[153] TV Globo от 2 сентября 2013 г.
[154] Der Spiegel от 20 октября 2013 г.
[155] The Guardian от 17 июня 2013 г.
[156] The Guardian от 17 июня 2013 г.
[157] The Guardian от 6 августа 2013 г.

Интернет.[158] С помощью специальной программы АНБ способно получать доступ к файлам, хранящимся на компьютерах пользователей, их паролям и сведениям об их Интернет-деятельности (рис. 6.3.)[159].

Рис. 6.3.

6.3. Кибернаступление США

Анализ документов показывает, что в 2011 г. спецслужбы США совершили 231 наступательную кибероперацию. Три

[158] Луковая маршрутизация (Onion routing) - технология анонимного обмена информацией через компьютерную сеть. Сообщения неоднократно шифруются и потом отсылаются через несколько сетевых узлов, называемых луковыми маршрутизаторами. Каждый маршрутизатор удаляет слой шифрования, чтобы открыть трассировочные инструкции и отослать сообщения на следующий маршрутизатор, где все повторится. Таким образом, промежуточные узлы не знают источника, пункта назначения и содержания сообщения. На 2009 год анонимная сеть Tor является доминирующей технологией, которая использует луковую маршрутизацию.

[159] The Guardian от 4 октября 2013 г.

четверти из них были направлены против Ирана, России, Китая и Северной Кореи. К концу 2013 г. планировалось поставить под американский контроль 85 000 стратегически отобранных компьютеров по всему миру, для их последующего вывода из строя[160]. Всего же АНБ выделило 61 000 целей для проведения наступательных кибероперациий по всему миру[161].

В апреле 2013 г. **АНБ создало тайный список своих основных «мишеней». Среди них Китай, Россия, Иран, Пакистан, Северная Корея, Афганистан, Германия и другие страны, а также Евросоюз.** При этом все страны оцениваются по шкале от 1 до 5, где 1 – высший приоритет для АНБ. Из европейских государств наибольший интерес для США – Германия.[162]

Анализ киберпрограмм США показывает, что американские военные все больше фокусируются на развитии ударных возможностей в информационном пространстве. Согласно опубликованному «секретному бюджету» американских спецслужб, в 2013 г. из федерального бюджета на нужды разведки было выделено 52,6 млрд. долл. Больше всего средств запросило ЦРУ - 14,7 млрд. долл., АНБ - 10,8 млрд. долл. и Национальное управление военно-космической разведки США - 10,3 млрд. долл. Основные статьи расходов: предупреждение американских властей об угрозах, борьба с терроризмом, противодействие распространению оружия, проведение активных спецкибероперациий и контрразведка[163]. Приоритетом контрразведки определено противодействие разведдеятельности Китая, России, Кубы, Пакистана, Ирана и Израиля.[164]

В октябре 2012 г. была издана секретная директива президента США, согласно которой, наступательные операции в информационном пространстве предоставляют

[160] The Washington Post от 31 августа 2013 г.
[161] The South China Morning Post от 11 сентября 2013 г.
[162] Der Spiegel от 26 августа 2013 г.
[163] The Washington Post от 29 августа 2013 г.
[164] The Washington Post от 29 августа 2013 г.

исключительные возможности для США продвигать свои национальные интересы в глобальных масштабах[165]. Американским военным и разведслужбам поручено подготовить план с указанием списка целей, против которых будет применяться кибероружие.

В рамках проекта «План икс» в США создается карта мирового информационного пространства в режиме реального времени. При этом операции будут осуществляться, естественно, без предупреждения объекта нападения.

Планом предусматривается уничтожение информационной инфраструктуры противника, в частности вывод из строя компьютерных систем критически важных объектов.

В случае неотвратимости кибернаступления противника предусматривается нанесение превентивного удара. В директиве заложена возможность проведения таких операций и в информационном пространстве США, но только после указания президента.

6.4. «Цифровой фашизм» спецслужб США?

Опубликованные документы убедительно показывают, что спецслужбы США имели доступ практически к каждому пользователю Интернета. Особое место отводилось государственным, дипломатическим, экономическим и иным чувствительным источникам информации. Так, АНБ следило за 38 посольствами и миссиями, в том числе представительствами ЕС в Нью-Йорке и Вашингтоне и штаб-квартирой МАГАТЭ в Вене. При этом наряду с идеологическими противниками США и странами Ближнего Востока в этот список попали посольства Франции, Италии, Греции, Японии, Мексики, Южной Кореи и Турции[166].

[165] The Guardian от 7 июня 2013 г.
[166] The Guardian от 30 июня 2013 г.

При этом АНБ осуществляет сбор персональных данных на территории США, что запрещено национальным законодательством. Действуя с разрешения американского суда по делам о надзоре за деятельностью иностранных разведслужб, АНБ перехватывает до 75% всех Интернет-коммуникаций в стране[167].

С 2001 по 2011 гг. в США по разрешению суда функционировала программа «Stellar Wind» по сбору так называемых «метаданных». Вначале собирались данные о телефонных звонках, совершенных из США за границу или в пределах США абонентов, которые не являлись американскими гражданами. Однако позднее АНБ получило полномочия собирать данные и о гражданах США[168]. В 2007 г. под контролем спецслужб оказалось около 34 тысяч человек, включая 3 тысячи граждан США.

Характерно, что с 2008 г. АНБ отслеживает всю Интернет-деятельность граждан США, подозреваемых в связях с иностранцами. Официально программа была разрешена секретной директивой № 424 в ноябре 2010 г. При этом АНБ использует компьютерные алгоритмы для создания детальных схем контактов и поведения американцев. Информация берется как из открытых, так и конфиденциальных источников и сохраняется на специальных серверах до года[169]. **Программа способна перехватывать 20 млрд. «событий» в день и обрабатывать их за 1 час.**

Важным инструментом геоинформационного господства США является программа «XKeyscore». Она способна мониторить практически все действия пользователей в сети Интернет, собирать о них все сведения, включая содержание электронных писем и переписку в соцсетях. В докладе АНБ от 2007 г. говорится о том, что в рамках программы была собрана информация о 850 млрд. телефонных звонках и

[167] The Wall Street Journal от 20 августа 2013 г.
[168] The Guardian от 27 июня 2013 г.
[169] The Guardian от 30 сентября 2013 г.

150 млрд. электронных записях. Ежедневно в эту базу данных добавлялось 1-2 млрд. записей.

В 2012 г. в течение месяца этой программой было собрано 41 млрд. записей[170].

«X-Keyscore» - секретная программа компьютерного слежения, осуществляется совместно АНБ США, Управлением радиотехнической обороны Австралии и Службой безопасности правительственных коммуникаций Новой Зеландии. Предназначена для слежения за иностранными гражданами во всем мире, деятельность осуществляет с помощью более чем 700 серверов, расположенных в США и на территории стран-союзников США, а также в посольствах и консульствах США в нескольких десятках стран, в том числе в Москве, в Киеве и Пекине. [171]

Ниже приводятся слайды из секретной презентации о программе, её глобальном размещении и функционале (рис. 6.4., 6.5.).[172]

[170] The Guardian от 31 июля 2013 г.
[171] http://top.rbc.ru/politics/12/08/2013/869734.shtmlhttp://top.rbc.ru/politics/12/08/2013/869734.shtml Э.Сноуден: Сервер-шпион американских спецслужб находится в Москве
[172] http://www.slideshare.net/xkeyscore/xkeyscore-nsa-program-presentation 18.12.2013

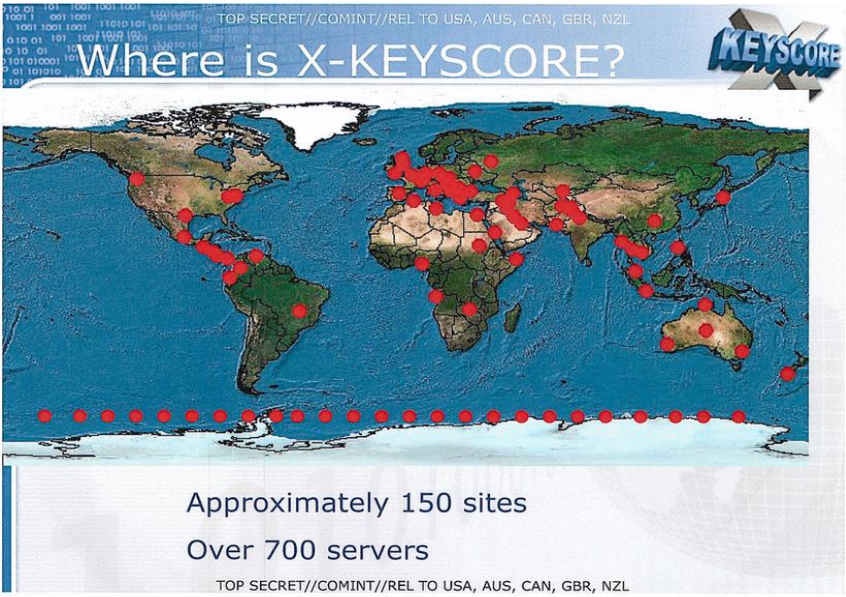

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Where is X-KEYSCORE?
KEYSCORE
Approximately 150 sites
Over 700 servers
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Рис. 6.4.

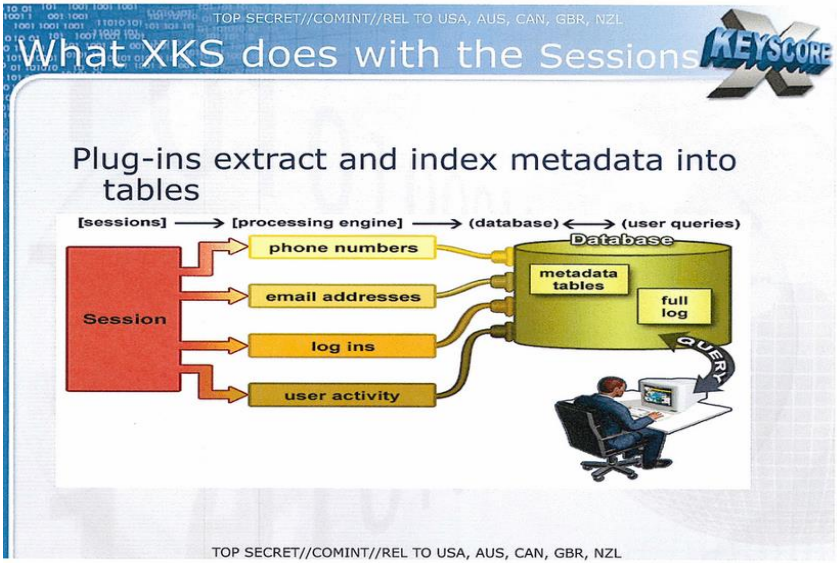

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
What XKS does with the Sessions
KEYSCORE
Plug-ins extract and index metadata into tables
[sessions] → [processing engine] → (database) ↔ (user queries)
Session
phone numbers
email addresses
log ins
user activity
Database
metadata tables
full log
QUERY
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Рис. 6.5.

При этом «X-Keyscore» способна сохранять несколько дней метаданные и контент перехваченных сообщений.[173]

Следует подчеркнуть, что «XKeyscore» выявляет гражданство иностранцев, анализируя язык, используемый в сообщениях электронной почты, перехваченной в странах Латинской Америки, особенно в Колумбии, Эквадоре, Венесуэле и Мексике[174].

С 2010 г. АНБ отслеживало международные платежи частных лиц, в том числе по пластиковым картам «Visa», и составило собственную базу данных. В 2011 г. в ней содержалось 180 млн. записей, 84% из них – по транзакциям с помощью кредитных карт. АНБ мониторило данные по транзакциям через международную банковскую систему «Swift» и шпионило за держателями кредитных карт в Европе, на Ближнем Востоке и в Африке.

Кроме того, с 2006 г. АНБ получило доступ к внутренним коммуникациям трех крупнейших мировых авиакомпаний, в том числе и к системе бронирования российской компании «Аэрофлот». И, наконец, американские спецслужбы и ведомства осуществляли слежку за арабским телеканалом «Al Jazeera» и другими СМИ.

6.5. ИКТ – гиганты на «спецслужбе» США

Благодаря умышленно заложенным в поставляемое программное обеспечение «лазейкам» АНБ способно взломать любую систему его защиты, созданную американскими ИКТ-компаниями. Так, компания «Microsoft» в течение последних трех лет предоставляла доступ американским спецслужбам к сообщениям пользователей и возможность обходить соб-

[173] German Intelligence Agencies Used NSA Spying Program — SPIEGEL ONLINE 18.12.2013

[174] O Globo от 6 июля 2013 г.

ственную криптографическую защиту для перехвата писем и чатов почтового клиента «Outlook».

С 2013 г. «Microsoft» сотрудничала с ФБР с тем, чтобы облегчить АНБ доступ через программу «Prism» к облачному хранилищу файлов «SkyDrive» (им пользуется более 300 млн. чел).

Данные, полученные программой «Prism», направлялись также в ФБР и ЦРУ. При этом число прослушиваний «Skype» возросло в три раза, начиная с июля 2012 г., то есть через 9 месяцев после того, как компания «Microsoft» купила «Skype»[175].

Компания «Verizon» по требованию американского суда предоставляла АНБ данные (местоположение звонившего, телефонные номера абонентов, длительность разговора) о телефонных переговорах американских граждан[176].

Характерно, что спецслужбы США используют сверхмощные компьютеры для взлома кодов и сотрудничают с некоторыми технологическими компаниями в США и за рубежом для создания своей «точки входа» в их продукты[177]. Так, проект «Bullrun» позволяет АНБ заниматься криптоанализом. При этом возможности США по декодированию известны лишь ограниченному кругу ведущих аналитиков из государств объединения «Пять глаз» (на сами эти страны программа «Bullrun» не распространяется).

6.6. Партнеры и объекты слежки спецслужб США

6.6.1. Великобритания - главный «спецпартнер» США

Британский Центр правительственной связи (ЦПС) – главный партнер спецслужб США. В рамках секретной про-

[175] The Guardian от 12 июля 2013 г.
[176] The Guardian от 6 июня 2013 г.
[177] O Globo от 6 июля 2013 г.

граммы «Tempora» ЦПС тесно сотрудничал с такими компаниями, как «British Telecom», «Vodafone Cable», «Global Crossing», «Verizon Business», «Level 3», «Viatel» и «Interut»[178].

Компании предоставляли спецслужбам неограниченный доступ к оптоволоконным кабелям, по которым передаются данные о содержании телефонных переговоров, электронных писем и сообщений пользователей в социальной сети «Facebook». В качестве компенсации им выплачивались денежные средства для поддержания своих сетей в исправном состоянии (394 млн. долл. - в 2011 г., 278 млн. долл. – в 2013 г.). Эти деньги выделялись на программы по сбору данных «Fairview» (94 млн. долл.), «Blarney» (65 млн. долл.), «Stormbrew» (46 млн. долл.), «Oakstar» (9 млн. долл.).

Информация хранилась на серверах ЦПС в течение 30 дней, а длительность работы самой программы составила как минимум 20 месяцев. Спецслужбы ежедневно получали в свое распоряжение свыше 600 млн. телефонных переговоров, имели доступ к 200 оптоволоконным кабелям, соединяющим Европу и Америку, с пропускной способностью до 10 гигабайт в секунду (контролируя одновременно до 46 кабелей). За это время была собрана информация о 2 млрд. пользователях сети Интернет. ЦПС инвестировала в программы, позволяющие получать личную информацию из мобильных телефонов и приложений. **Анализ показывает, что ЦПС превосходит АНБ по количеству отслеживаемой информации.**

Характерно, что за период с 2010 г. США выплатили ЦПС около 160 млн. долл. за возможность получать доступ к британским разведывательным программам и влиять на них[179]. При этом АНБ оплачивает половину стоимости одной из разведывательных систем Великобритании, расположенных на Кипре[180].

---

[178] The Guardian от 21 июня 2013 г.
[179] The Guardian от 1 августа 2013 г.
[180] The Guardian от 2 августа 2013 г.

Резюмируя, следует отметить, что ЦПС тесно сотрудничает с АНБ для обеспечения проведения британских и американских военных спецкибероперациий. При этом ЦПС становится все более финансово зависимой от американских источников: с 2006 г. по 2012 г. внешние дотации выросли с 23 млн. долл. до 244 млн. долл.[181]

6.6.2. Дилемма Германии – спецпартнер и спецобъект мониторинга США

18 июня 2014 г. издание Der Spiegel разместило на своем портале новую порцию разоблачительных материалов, которые предоставил Э.Сноуден - так называемое немецкое досье - 53 файла.[182] Журналисты пришли к выводу, что на европейском направлении самую активную деятельность американцы вели именно в Германии. На территории страны действовали более 100 пунктов сбора информации в интересах ЦРУ.

Der Spiegel отмечает, что эти данные могут оказаться полезными и для Ангелы Меркель, которая давно и безуспешно пытается получить немецкое досье из Вашингтона.

При этом, АНБ США с 2002 года собирало сведения о звонках канцлера Шрёдера по мобильному телефону и его СМС-переписке. Это связывают с тем, что тогдашний лидер Германии возражал против вторжения в Ирак. По информации радиостанции «Норддойче рундфунк», за политиком стали шпионить после того, как он второй раз был избран на пост канцлера. Сам Шредер заявил в прессе, что ничуть не удивлен.[183]

Выяснилось, что американская разведка тесно сотрудничала с коллегами в Берлине, проводила обучающие курсы и делилась секретными программами. Так, **немецкие спец-**

[181] The Guardian от 2 августа 2013 г.
[182] http://www.spiegel.de/netzwelt/netzpolitik/nsa-dokumente-von-snowden-enthuellen-standorte-in-deutschland-a-975611.html 20.06.2014
[183] http://www.ntv.ru/novosti/838389/ 20.06.2014

службы BND (внешняя разведка) и BfV (контрразведка) получили возможность использовать «X-Keyscore».[184]

В переданных документах BND была охарактеризована как один из самых успешных партнёров АНБ в сборе информации. Из примерно 500 млн. файлов, ежемесячно получаемых АНБ от коллег из ФРГ, порядка 180 млн. оказывались в доступе спецслужбы благодаря «X-Keyscore»[185].

Объем отслеживаемых данных, проходящих через один из крупнейших мировых узлов Интернет-траффика во Франкфурте-на-Майне, достигал 2,5 терабайтов в секунду.

Офисы «Yahoo» в Германии, как и ирландские офисы «Apple», «Facebook», «Microsoft» и «Skype» в Люксембурге, и предоставляли спецслужбам США с помощью программы «Prism» беспрепятственный доступ к персональной информации граждан ЕС[186]. При этом США следили за немецкими компаниями в интересах американской экономики. Ежегодный ущерб от американской прослушки оценивается от 30 до 60 млрд. евро.

В ответ на американскую «киберэкспансию» в июле 2013 г. канцлер ФРГ А.Меркель предложила выработать по линии ЕС стратегию развития ИКТ. На саммите ЕС главы государств и правительств 28 европейских стран приняли специальное заявление, в котором выразили озабоченность действиями США[187].

Германия и Франция выступили с инициативой вступить в двусторонние переговоры с США с целью решения проблемы прослушивания телефонных переговоров путем заключения с Вашингтоном некоего «пакта о недопустимости слежки» друг за другом. [188]

---

[184] http://top.rbc.ru/society/21/07/2013/866925.shtml СМИ: Разведка ФРГ применяла шпионскую программу АНБ 18.12.2013
[185] Der Spiegel от 20 июля 2013 г.
[186] Der Spiegel от 10 июня 2013 г.
[187] Interfax от 25 октября 2013 г.
[188] BBC от 25 октября 2013 г.

К 2018 г. ФРГ планирует увеличить число сотрудников в отделе технической разведки и технического переоснащения БНД, вложив в нее 100 млн. евро. При этом правительство ФРГ аннулировало 2 августа 2013 г. так называемые административные соглашения от 1968/1969 гг. с США и Великобританией.

В МИД ФРГ летом 2013 г. был введен пост уполномоченного по вопросам информационной безопасности. Его занял 57-летний дипломат Дирк Бренгельман, главной задачей которого определено обеспечение защиты информационных сетей и свободы в Интернете.

Характерно, что 28 августа 2013 г. по инициативе Федерального ведомства по охране конституции полиция ФРГ произвела в воздушную съемку здания Генконсульства США во Франкфурте-на-Майне и прилегающей к нему территории, так как именно через этот узел американские спецслужбы перехватывали наибольший объем информации.

6.6.3. Латинская Америка – «кибервотчина» США

АНБ имело доступ к миллиардам электронных писем и телефонных звонков стран Латинской Америки. Особое значение придавалось Бразилии. Под прикрытием сотрудничества американских и бразильских телекоммуникационных компаний (в т.ч. местное подразделение «Google», отделение бельгийской компании «Swift»)[189] АНБ следило за деятельностью крупных частных и государственных компаний, в том числе «Petrobraz», по таким стратегически важным вопросам, как организация тендеров, разработка нефтяных месторождений, проекты в оборонной сфере.

Участник системы «Эшелон» Канадский Центр безопасности коммуникаций совместно со спецслужбами США участвовал в шпионаже против Министерства горнодобыва-

[189] TV Globo от 9 сентября 2013 г.

ющей промышленности и энергетики Бразилии. Шпионаж осуществлялся с помощью компьютерной программы «Олимпия» в интересах частных компаний[190]. Канадские спецслужбы интересовались схемами коммуникаций министерства, перехватывая телефонные разговоры, переговоры и электронную переписку чиновников и самого министра. Отчет о результатах проделанной работы был представлен Канадой в июне 2012 г. на закрытой конференции представителей государств-членов объединения спецслужб «Эшелон» («Пять глаз»).

Комиссия сената Бразилии по расследованию фактов шпионажа спецслужб США заслушала проживающего в Бразилии английского журналиста Г.Гринвальда. Именно ему в свое время Э.Сноуден передал разоблачительные документы. Публикации в СМИ на основе этих документов вскрыли факты слежки спецслужб за телефонными переговорами и электронной перепиской президента Бразилии Дилмы Роуссефф, бразильских дипломатов, сотрудников стратегически важных министерств и компаний южноамериканской страны.

Разоблачительные материалы о деятельности американских спецслужб против Бразилии стали причиной охлаждения в отношениях между двумя странами. Глава бразильского государства с трибуны Генассамблеи ООН выступила с резкой критикой шпионской деятельности и выдвинула инициативу создать механизмы гражданского контроля над Интернетом с целью обеспечить безопасность пользователей, не ограничивая их права на свободный доступ к ресурсам сети.

В открытом письме Сноудена, адресованном народу и властям Бразилии, он отмечает, что был впечатлен резкой критикой деятельности американских спецслужб и шпионажа со стороны США, а также выразил готовность помочь Бразилии расследовать слежку АНБ в обмен на политическое убежище.[191]

---

[190] Toronto Star от 7 октября 2013 г.
[191] http://ria.ru/world/20131217/984619539.html#ixzz2nnVXU6I8 21.06.2014

Бразилия предприняла шаги для снижения зависимости от американских Интернет-компаний и сервисов, т.е. укреплению информационного суверенитета. Принято решение о развитии национальной системы электронной почты (с планами стать сервером автономной региональной сети), укреплении безопасности правительственной связи, реформе национального законодательства – введении обязательного правила хранения электронных баз данных на территории страны, отзыве лицензий у компаний, уличенных в пособничестве кибершпионажу.

Намечено ужесточить контроль над использованием зарубежного технического оборудования, увеличить ответственность операторов и технического персонала, минимизировать закупки американских комплектующих и элементной базы для важных информационных систем.

В 2014 г. предусматривается создание Центра контроля трафика сети Интернет в г.Форталеза. В 2014-2015 гг. правительство намерено осуществить запуск национального спутника связи и проложить две оптоволоконные линии коммуникаций (одна для связи со странами Карибского бассейна и рядом европейских государств, а вторая – с Африкой).

Тема МИБ стала приоритетной для Бразилии. Бразилия намерена также усилить работу по управлению сетью Интернет и активизировать деятельность рабочей группы, созданной в соответствии с резолюцией ГА ООН A/Res67/195.[192] Глобальная многосторонняя конференция о будущем управления Интернетом прошла в Сан-Пауло 23-24 апреля 2014 года.[193]

13 сентября 2013 г. министры обороны Бразилии и **Аргентины** подписали соглашение о совместных шагах по противодействию кибершпионажу со стороны США.

---

[192] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N12/490/32/PDF/N1249032.pdf?OpenElement 21.06.2014

[193] https://www.icann.org/news/announcement-2014-01-11-ru 21.06.2014

Эквадор на полях сессии Совета ООН по правам человека провел встречу, посвященную «разоблачителям» нарушений прав человека и связанными с этим правовыми и нравственными проблемами, на которой виртуально из посольства в Лондоне участвовал основатель «Wikileaks» Дж.Ассанж.

6.6.4. Особая роль Франции

АНБ вело широкомасштабную слежку за Францией. Только за период с 10 декабря 2012 г. по 8 января 2013 г. АНБ перехватило 70,3 млн. телефонных разговоров французских граждан, представителей политической и деловой элиты страны, сотрудников министерств и ведомств. Также перехватывалась электронная переписка пользователей, которая обрабатывалась компаниями «Wanadoo» и «Alcatel-Lucent»[194].

Особая роль Франции заключается в том, что она создала и использует собственную систему «Frenchelon» - аналог «Эшелона» и PRISM. (рис. 6.6.).[195]

[194] Le Monde от 21 октября 2013 г.
[195] Le Monde от 4 июля 2013 г.

Рис. 6.6.

6.6.5. Другие страны - «спецобъекты» США

Швеция является одним из секретных партнеров АНБ США и тесно сотрудничает с США и Великобританией в деле тотальной прослушки. Радиокоммуникационная служба шведской обороны (FRA) снимает информацию с подводных кабелей, осуществляя слежку за странами Балтии и за российскими фирмами и передавая информацию АНБ.

Зафиксировано 9 случаев несанкционированного или необоснованного сбора, хранения, обработки и воссоздания чувствительной или неоправданно подробной информации, в том числе о физических лицах, недопустимого использования поисковых понятий, недостаточной отчетности и ведения документации, затрудняющей контроль.

Индия. С помощью программ «Boundless Informant» и «Prism» американские спецслужбы осуществляли слежку за Индией, перехватывая информацию о внутренней политике,

стратегических и коммерческих интересах страны, ее ядерной и космической программах и т.д. АНБ наблюдало за государственными учреждениями страны и чиновниками различного уровня, учеными и другими лицами, представляющими интерес для США. Слежка велась за индийской миссией ООН в Нью-Йорке и Посольством Индии в Вашингтоне.

Следует отметить, что у Индии имеется Национальная разведывательная сеть NATGRID (акроним англ. National Intelligence Grid), которая консолидирует базы данных нескольких министерств и ведомств, для облегчения спецслужбам Индии оперативного доступа к требуемой информации. Идея создания NATGRID возникла после терактов в Мумбаи в 2008 г.[196]

Италия. Британские и американские разведывательные службы в массовом порядке ведут мониторинг телефонных сообщений, в том числе военного и коммерческого характера, и Интернет-трафика в Италии.[197]

Нидерланды. В декабре 2012 - январе 2013 гг. в рамках программы «Boundless Informant» АНБ прослушало телефоны около 2 млн. граждан.[198]

Бельгия. Американские спецслужбы с 2011 г. следили за клиентами крупнейшего оператора связи Бельгии «Belgacom», перехватывая международные телефонные разговоры.

В этих целях британский ЦПС (GCHQ) через фальшивые аккаунты социальной сети LinkedIn внедрил шпионскую программу в сеть бельгийского оператора.[199] Было «заражено» 25 тысяч компьютеров компании. Больше всего США интересовались подразделением «Belgacom» - «Bics», которое обеспечивало международную связь по всему миру, отслеживались контакты с Йеменом, Сирией, Афганистаном, Анголой, Демо-

[196] http://ru.wikipedia.org/wiki/NATGRID 21.06.2014
[197] Espresso от 24 октября 2013 г.
[198] Dutch news от 21 октября 2013 г.
[199] http://www.interfax.ru/world/txt/341907 18.02.2014

кратической Республикой Конго и еще рядом стран, к которым разведка США проявляет особый интерес[200].

В силу этого Министр иностранных дел Бельгии Д.Рейндерс и внес предложение о приостановке процесса подписания документа о трансатлантическом сотрудничестве по вопросам торговли и инвестиций с США до выяснения всех обстоятельств дела.

Израиль. США делятся с израильскими разведывательными службами необработанными разведданными, которые могут включать в себя конфиденциальную информацию об американских гражданах. Об этом стало известно из «Меморандума о взаимопонимании», заключенного между АНБ и его израильским аналогом[201].

Следует подчеркнуть, что боевой кибервирус «Stuxnet», поразивший компьютеры на иранской АЭС в Бушере, был разработан США совместно с Израилем[202].

Китай. АНБ проникло на серверы ряда китайских мобильных телефонных компаний и читало миллионы текстовых сообщений. АНБ взломало десятки компьютеров в престижном университете Циньхуа в Пекине и компьютеры «Pacnet» – крупнейшей телекоммуникационной компании со штаб-квартирами в Гонконге и Сингапуре. Учитывая это обстоятельство, КНР создала систему защиты «Золотой щит».[203]

Пакистан. Спецслужбы США осуществляли компьютерную слежку за Пакистаном, в частности, за программой пакистанского ядерного оружия. [204]

Характерно, что американский спецназ, участвовавший в операции по ликвидации Усамы бен Ладена, получал команды со спутников, которые передавали сигнал через специальные приемники, находившиеся на территории Пакистана[205].

---

[200] De Standaard от 16 сентября 2013 г.
[201] Los Angeles Times от 11 сентября 2013 г.
[202] The Register от 8 июля 2013 г.
[203] The South China Morning Post от 11 сентября 2013 г.
[204] The Washington Post от 2 сентября 2013 г.
[205] The Washington Post от 29 августа 2013 г.

Австралия. АНБ сотрудничало с Управлением радиотехнической обороны Австралии и Службой безопасности правительственных коммуникаций Новой Зеландии для реализации программы «XKeyscore»[206].

Австралийская компания «Telstra» сотрудничала с правительством США, храня информацию о звонках, совершенных между США и другими странами. Соглашение было подписано в 2001 г. и, по сути, давало компании возможность отслеживать содержание разговоров абонентов[207].

Норвегия. По данным газеты Dagbladet со ссылкой на документы, обнародованные Э.Сноуденом,[208] за период с 10 декабря 2012 г. по 8 января 2013 г. АНБ перехватило на территории страны 33 млн. звонков, что составляет 10% от всего трафика мобильной связи в Норвегии. Таким образом, **Норвегия оказалась страной, в которой американцы отследили наибольшее количество данных в соотношении с количеством жителей**.

Следует отметить, что все три спецслужбы Норвегии на следующий день после публикации отклонили утверждения газеты. [209]

Символично, что Э.Сноуден был выдвинут норвежцами кандидатом на Нобелевскую премию мира.[210]

6.7. Международное сообщество - за неприкосновенность личной жизни в цифровой век

С учетом волны возмущения противоправной деятельностью спецслужб США Германия и Бразилия в конце октября

[206] The Sydney Morning Herald от 8 июля 2013 г.
[207] The Guardian от 12 июля 2013 г.
[208] Dagbladet 19.11.2013
[209] http://www.interfax.ru/world/txt/341907 20.06.2014
[210] http://www.dagbladet.no/2014/06/22/nyheter/politikk/edward_snowden/nobels_fredspris/fredsprisen/33969325/ 22.06.2014

2013 г. внесли в ООН проект резолюции, которая распространила бы на Интернет право на невмешательство в частную жизнь, закрепленное в Международном пакте о политических и гражданских правах.

19.12.2013 ГА ООН консенсусом одобрила резолюцию «Право на неприкосновенность личной жизни в цифровой век».[211]

Генассамблея подтвердила, что **те же права, которые человек имеет в офлайновой среде, должны также защищаться и в онлайновой среде, особенно право на неприкосновенность личной жизни.**

Кроме того, в документе содержится призыв Генассамблеи к государствам «провести обзор процедур, практики и законодательства, касающихся слежки за сообщениями, их перехвата и сбора личных данных». Также в принятой резолюции есть призыв к Верховному комиссару ООН по правам человека подготовить доклад о защите права на неприкосновенность личной жизни. [212]

6.7.1. Вассенарские соглашения: продажа кибероружия будет сокращена

Инструменты наблюдения, средства вторжения и технологии для защиты от них активно разрабатываются частными компаниями разных стран мира. По оценке британского Агентства по торговле и инвестициям (UKTI), оборот мирового рынка средств кибербезопасности составляет 123 млрд. фунтов стерлингов ($201 млрд.) и растет ежегодно на 10%.

Правительства 41 страны, подписавшей Вассенарские соглашения (США, Великобритании, России и большинства стран ЕС), намерены ограничить продажи систем слежения за Интернет-трафиком, а также средств программного вторжения, которые обычно используют спецслужбы. **Под действие**

[211] http://www.un.org/russian/news/story.asp?NewsID=20792 21.06.2014
[212] https://www.un.org/russian/news/story.asp?NewsID=20669 18.12.2013

соглашения подпадает любое программное обеспечение для сбора метаданных.[213] Ограничивается и продажа программ для отслеживания действий пользователей в Интернете. Участники соглашения признали, что необходимо усилить контроль над программами, позволяющими «определять схемы отношений отдельных людей и групп». Исключение делается для компаний, использующих эти технологии для маркетинга или изучения поведения потребителей.

Жесткие ограничения накладываются также на распространение определенных типов вредоносного софта, способного причинить ущерб компьютерам, сетям или оборудованию, управляемому с компьютера.

Западные спецслужбы особенно озабочены возможностью попадания потенциально опасных технологий в руки террористов и боевиков. Великобритания с 2014 года ввела правила, обязывающие все компании, ведущие бизнес с правительством, обеспечить соблюдение стандартов кибербезопасности во всех цепочках субподрядчиков. В декабре 2013 г. премьер-министр Великобритании Д.Кэмерон во время своего визита в Китай (не подписавший Вассенарские соглашения) сообщил о возможном начале переговоров между двумя странами по кибербезопасности.

В мире растет понимание и поддержка действий Сноудена по разоблачению тотальной слежки в Интернете спецслужб США и их союзников. Подтверждением этому стало его номинирование на Нобелевскую премию мира, а также присуждение ему ряда премий.

Так, 22 июня 2014 г. Э.Сноуден получил от общественной организации «Гуманистический союз» ФРГ символическую премию за гражданское мужество.[214]

---

[213] http://www.vedomosti.ru/tech/news/20286881/prism-priznali-kiberoruzhiem#ixzz2nl3npzQy 17.12.2013

[214] http://izvestia.ru/news/572773 22.06.2014

Знание действия зависит от знания причины
и заключает в себе последнее.
(Б. Спиноза)

7. ИННОВАЦИОННЫЕ МЕТОДЫ АНАЛИЗА ВО ВНЕШНЕЙ ПОЛИТИКЕ

7.1. Краткий обзор традиционных методов

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.**

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.**

7.1.1. 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).

Возведя Россию в ранг сердцевины земного шара (Хартленда), основатель геополитики Маккиндер сделал вывод о том, что без контроля над Хартлендом (Россией) мировое господство англосаксов невозможно.[215]

«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»[216].

Многие аналитики используют данный закон для объяснения причин глобальных конфликтов.

Другой составляющей геополитического подхода являются внутренние аспекты объекта исследования: политическая система государства, социально-экономический, военный, научно-технический, информационный потенциал, этноконфессиональный состав и т.д.

---

[215] См. http://www.mstu.ru/forum/index.php?topic=21092.0

[216] Mackinder H. Democratic ideals and reality, New York, 1919. P. 34.

7.1.2. 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.**

7.1.3. Интерактивный подход

Интерактивный подход рассматривает взаимодействие на уровне государств и иных субъектом межгосударственных отношений. Его суть можно изобразить в виде следующей схемы 7.1.

Схема 7.1.

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**.

7.1.3.1. 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 (схема 7.2.):

Схема 7.2.

		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.

7.1.3.2. Теория торга

По теории торга (по В.Зартману)[217] 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.**

7.1.3.3. 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

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

поведения государств описывается с помощью дифференциальных уравнений[218].

Ниже приводится классификационная таблица 7.1. основных методов взаимодействия участников внешнеполитических процессов[219].

Таблица 7.1.

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
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)

[218] 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

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

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

7.1.4. Основные понятия системного подхода

Системный подход интегрирует основные аспекты предыдущих подходов и широко используется в конфликтологии с середины 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»[220], 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 (вспомним еще раз Б.Спинозу!).

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.

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.

---

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

7.1.5. 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.

7.1.6. Типы и способы урегулирования конфликтов

В конце XX в. Ф.Брайар и М.Р.Джалили выдвинули основанную на системном подходе концепцию детерминант внешней политики. Её суть состоит в том, что **внутренние и внешние факторы воздействуют на внешнюю политику государства, тесно взаимодействуя друг с другом**[221].

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 мас-

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

штабы 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-переговорный 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.

7.1.6.1. 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 дипломатических служб и т.п.

7.2. 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»**[222]**.**

[222] 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

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[223].

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).

7.2.1. 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;
- 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

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

свое содержание и структуру, и может исследоваться как конфликтная ситуация.

Эскалационное развитие конфликта включает следующие фазы[224]:

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.

---

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

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 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.**

7.2.2. 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[225].

[225] 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

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;
- 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**[226], 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.

---

[226] 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[227]:

- 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 п.7.5.). Информация характеризуется двумя основными факторами - это степень ее достоверности и сведений о содержании и значении признаков и показателей собранной информации.

Матрица размещения компонентов конфликта, предло-

[227] 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

женная И.С.Бабинцевым[228], 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 одного 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 (табл. 7.2.).

Таблица 7.2.

Ранги 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

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

Степень важности	Определение	Пояснения
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	

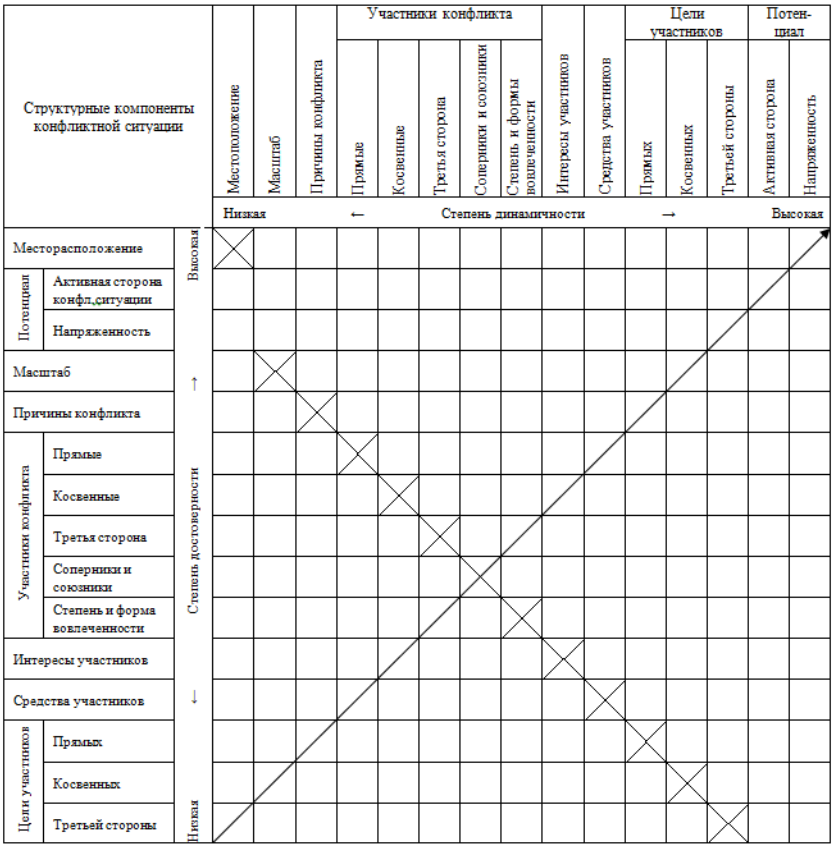
Далее по таблице составляется матрица сравнений[229], которая необходима для создания формальной модели (схема 7.3.).

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.

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

Схема 7.3.

Матрица размещения компонентов конфликтной ситуации



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 участни-

ков», «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.

7.2.3. 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.

7.2.3.1. Конфликты согласно классификации ООН

Принцип мирного разрешения международных споров сформировался еще до второй мировой войны[230]. 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

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

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 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.**

7.2.3.2. 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[231].

7.2.3.3. 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**[232].

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.

---

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

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

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[233]. 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.

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

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

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**[234].

- 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.

---

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

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[235].

Направленность конфликтного поведения:

- соперничество (направленность на достижение целей, находящихся вне сторон);
- конфликт (направленность друг на друга);
- направленность поведения на цели оппонента.

Целесообразность открытой конфронтации для одной из сторон определяется формулой:

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 ответ-

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

ные 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 ве-

ка. 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.

7.2.3.4. 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[236]**:**

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 и 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.

Новая группа действующих лиц:

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

[236] Информационные войны рассмотрены в гл.3 и 4

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 ши-

рокого 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.

7.3. Современные методы анализа

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

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

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 членится 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.

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». 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 обстоятельство позволяет использовать данную методику не только для изучения конкретных проблем Северной Кореи и Ирака, но и в качестве конкретного пособия для формирования практических и аналитических навыков при проведении ситуационных анализов, в т.ч. с использованием современных ИКТ.

7.3.2. SWOT и STEEPLE-анализы

Метод SWOT-анализа, разработанный в рамках маркетинговых исследований в Гарвардской школе бизнеса в 1960-х гг.[237], и в настоящее время может использоваться и как самостоятельная методика, и как элемент ситуационного анализа. По своим исходным установкам SWOT-анализ является клиент-ориентированным: исследование ситуации происходит «под углом зрения» конкретного актора.[238]

---

[237] См. Andrews K. R., The Concept of Corporate Strategy (2nd ed.), Homewood et al. 1980.
[238] См. Ахременко, А. С. Политический анализ и прогнозирование : учеб. пособие / А. С. Ахременко.- М.: Гардарики, 2006. - 333 с.

Название метода - аббревиатура четырех английских слов[239]:

• Strength - сильные стороны;
• Weakness - слабые стороны;
• Opportunities - возможности;
• Threats - угрозы.

Первые две позиции - сильные и слабые стороны - факторы внутренней среды объекта анализа (то есть то, на что сам объект способен повлиять). Вторые две позиции - возможности и угрозы - факторы внешней среды (то есть то, что не контролируется объектом).

Схема 7.4.

Базовая матрица SWOT-анализа

Внутренняя среда	**Strengths** (свойства, дающие преимущества перед другими в отрасли)	**Weaknesses** (свойства, ослабляющие проект)
Внешняя среда	**Opportunities** (внешние вероятные факторы, дающие дополнительные возможности по достижению цели)	**Threats** (внешние вероятные факторы, которые могут осложнить достижение цели)

SWOT-анализ включает в себя: выявление экспертом наиболее важных параметров анализа, занесение их в матрицу таблицы и проведение их систематизации в каждой ячейке. Затем осуществляется общая оценка доминирования слабостей или позитивных характеристик. Толкование результатов - поиск конструктивных ответов на вопросы о возможностях преодоления слабостей и угроз и тех мер, которые необходимо применить.

Преимуществом SWOT-анализа является системная ха-

[239] P. Kotler, R. Berger, N. Bickhoff, The Quintessence of Strategic Management. What You Really Need to Know to Survive in Business, Springer 2010. P.30

рактеристика позиций актора по указанным выше признакам и комплексное рассмотрение сильных/слабых сторон актора через призму возможностей/угроз с использованием специальной матрицы SWOT-анализа[240] (схема 7.5.):

Схема 7.5.

	Возможности 1. 2.	Угрозы 1. 2.
Сильные стороны 1. 2.	Возможности и сильные стороны	Угрозы и сильные стороны
Слабые стороны 1. 2.	Возможности и слабые стороны	Угрозы и слабые стороны

Пересечение четырех разделов образует четыре дополнительных поля, позволяющих рассматривать характеристики позиций актора в разных сочетаниях. Одно из приоритетных значений имеет поле «Возможности и сильные стороны», определяющее наиболее перспективный стратегический вектор развития, а также поле «Угрозы и слабые стороны», показывающее наиболее уязвимые стороны позиции исследуемого объекта. Поле «Возможности и слабые стороны» демонстрирует, каким образом «проблемные» позиции могут быть компенсированы за счет новых возможностей. Поле «Угрозы и сильные стороны» позволяет лучше понять, каким образом ресурсные преимущества могут быть направлены на ликвидацию угроз.

SWOT-анализ все чаще применяется в связке с более современным методом **STEEPLE-анализа**. Последний включает в себя следующие факторы: социально-демографический (S), технологический (T), экономический (E), окружающая среда (природный) (E), политический (P), правовой (L) и эт-

[240] Ахременко, А.С. Политический анализ и прогнозирование : учеб. пособие /А. С. Ахременко. - М.: Гардарики, 2006. С. 264

нический (Е). При этом может учитываться и географический фактор.

Резюмируя, следует подчеркнуть, что наиболее эффективным из арсенала традиционных методов анализа, представляется комплексное использование ситуационного, а также SWOT и STEEPLE - анализов, ибо они позволяют креативно адаптировать полученные результаты к проблематике предмета и объекта исследования.

7.3.3. Методы прогнозирования международных конфликтов

7.3.3.1. 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[241]. 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 действия, прекращение военных действий, урегулирование. В рамках конфликта фазы могут сменять друг друга в любом направлении.

В фазово-факторной модели (рис. 7.1.) каждая фаза обладает параметром - **весом фазы** в конфликте[242], который пока-

[241] 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

[242] 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

зывает 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.

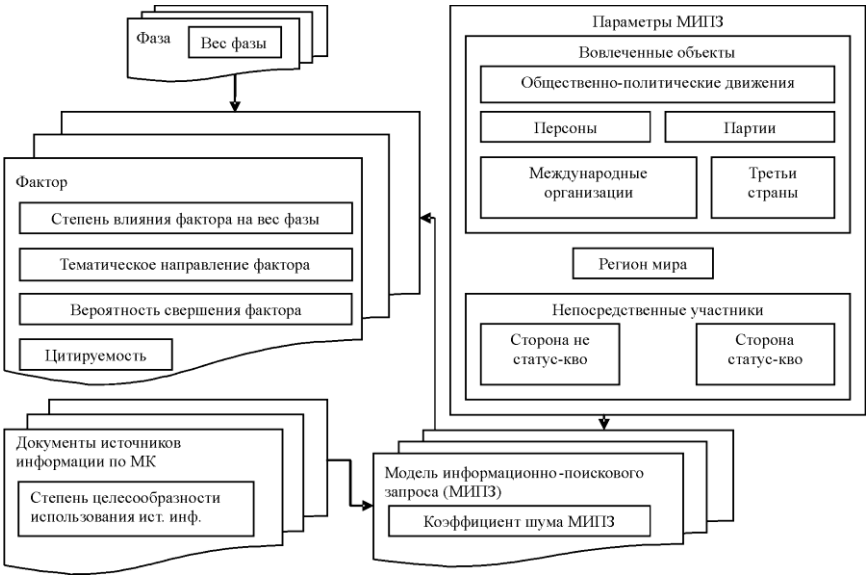


Рис. 7.1. Фазово-факторная модель международного конфликта

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 присут-

ствия 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 информации, 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.

7.4. Ситуационно-кризисный центр как инструментарий эксперта

В условиях роста конфликтного потенциала в мире резко возросла роль ситуационно-кризисных центров (СКЦ), оснащенных новейшими ИКТ.

Суть использования СКЦ заключается в возможности вести проблемный мониторинг, находить оптимальные варианты кризисного реагирования, а также моделировать и прогнозировать кризисы.

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.

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;

- 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.

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 подразделе-

ниями, 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.

7.4.2. 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, в т.ч. защищенных, использование которых позволяет привлекать удаленно находящихся экспертов.

При этом развивается направление оказания внешних (по отношению к владельцу СКЦ) услуг (outsourcing) организациями как для анализа проблемы, так и для использования их вычислительных мощностей. Перспективным видится использование «облачных» технологий с соответствующей системой обеспечения информационной безопасности.

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

7.4.3. Режимы работы ситуационно-кризисного центра

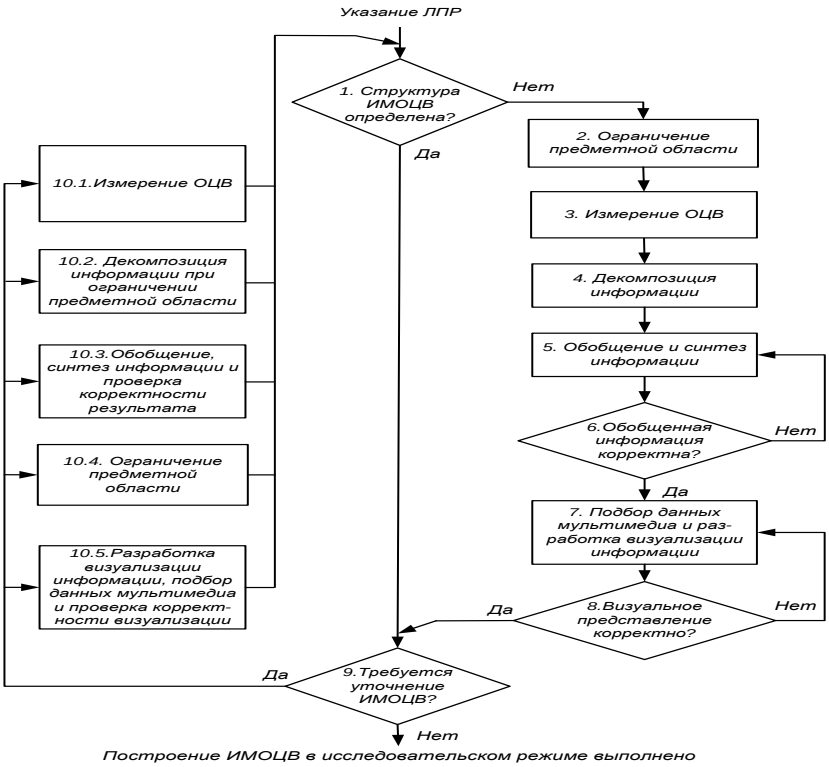
Как правило, в работе СКЦ выделяются следующие три режима.

7.4.3.1. Режим проблемного мониторинга

Мониторинг объекта целевого воздействия (ОЦВ) и информирование лица, принимающего решение (ЛПР), о достижения ОЦВ заданного состояния. Соответственно 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[243] работы:

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

Схема 7.6.

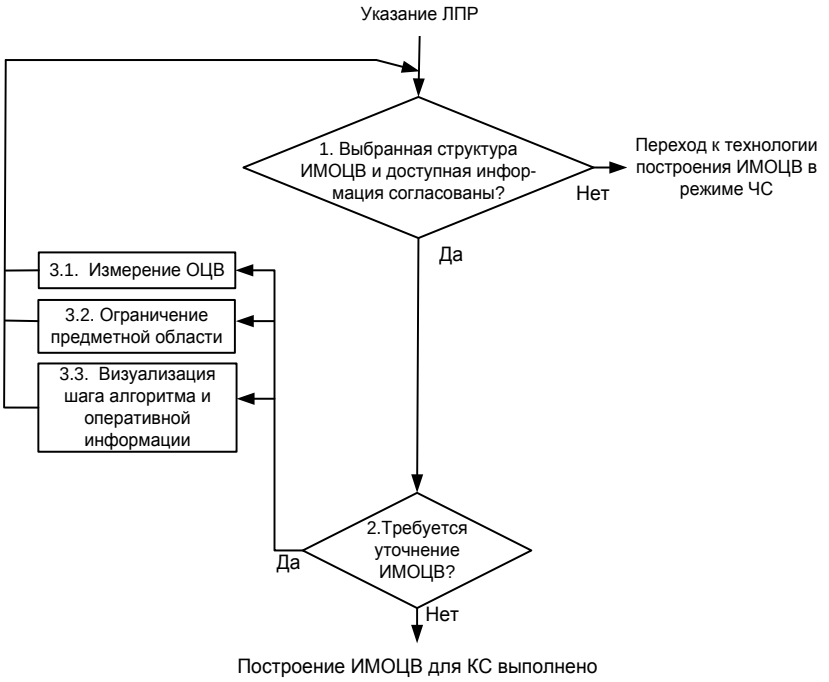


7.4.3.2. Режим кризисного реагирования

Режим кризисного реагирования, реализуемый в «онлайне», когда **на основе прецедентов и накопленной информации о фигурантах ситуации ИМОЦВ содержит готовые алгоритмы решений.** Схема[244] работы для кризисной ситуации (КС):

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

Схема 7.7.

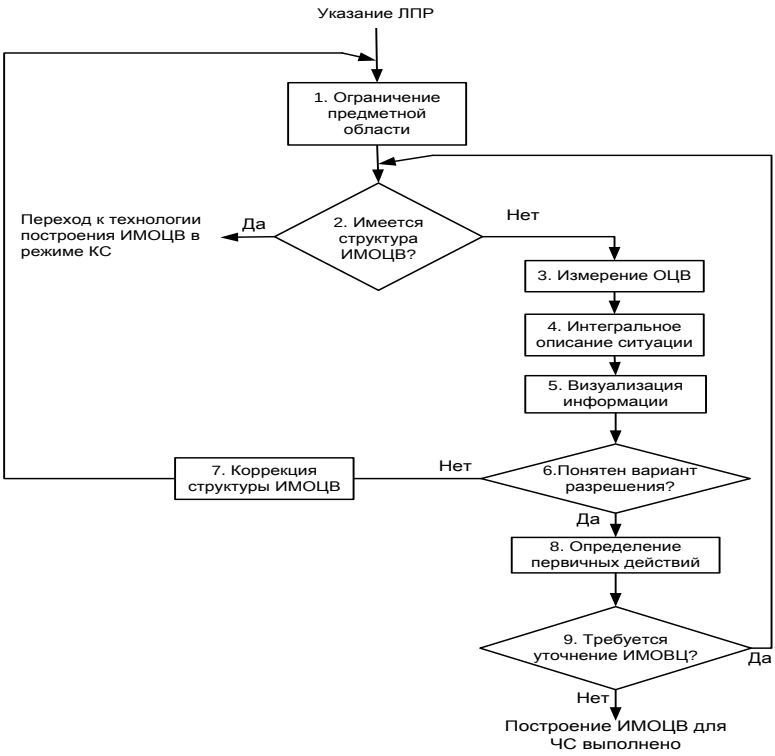


7.4.3.3. Режим чрезвычайной ситуации

Режим чрезвычайной ситуации протекает в «он-лайне». При этом, **в отличие от режима кризисной ситуации, нет знаний о прецедентах, нет готовых алгоритмов решения и лимит времени весьма ограничен**. Схема[245] работы в чрезвычайной ситуации (ЧС):

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

Схема 7.8.



Таким образом, СКЦ становятся неотъемлемой частью системы обеспечения международной безопасности.

7.4.1. Основные характеристики СКЦ МИД ФРГ и МИД Италии

СКЦ или их аналоги нашли широкое применение во внешнеполитическом процессе практически всех стран мира. Первым был создан Оперативный центр Госдепа США еще в 1961 г.

7.4.1.1. СКЦ МИД ФРГ

Центр кризисного реагирования (КЦ) МИД ФРГ структурно похож на Оперативный центр Госдепартамента США и занимает высокое место в иерархии министерства (рис. 7.2.)

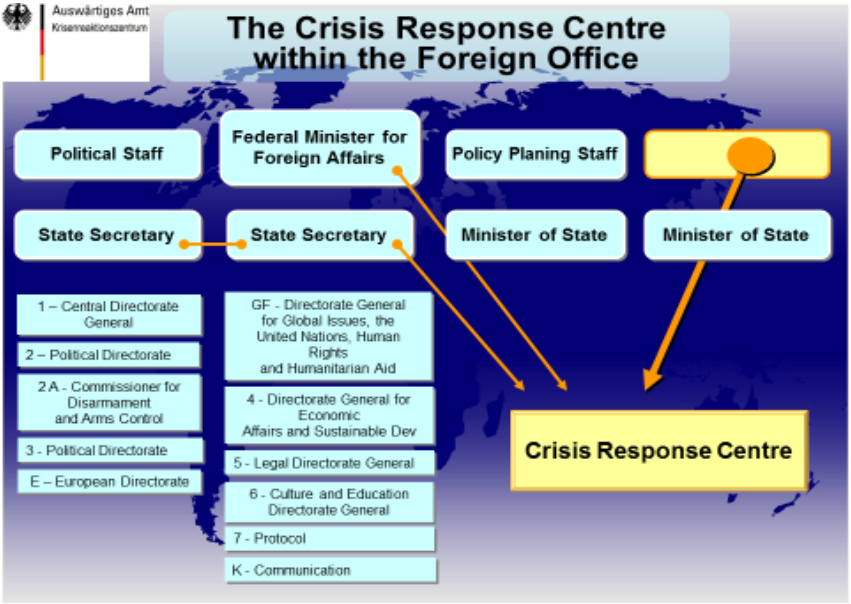


Рис. 7.2.

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 (рис. 7.3.), 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.

Рис. 7.3.

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 (рис. 7.4.).

Рис. 7.4.

Большое значение уделяется обучению персонала работе в кризисных ситуациях (рис. 7.5.).

Рис. 7.5.

В своей работе КЦ МИД ФРГ взаимодействует с КЦ других министерств и ведомств Германии, а также с ситуационным центром Евросоюза (рис. 7.6.).

Рис. 7.6.

7.4.1.2. СКЦ МИД Италии

СКЦ МИД Италии также достаточно высоко позиционирован в структуре министерства (рис. 7.7.).

Рис. 7.7.

Структура Кризисного центра (КЦ) МИД Италии (рис. 7.8.) 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.

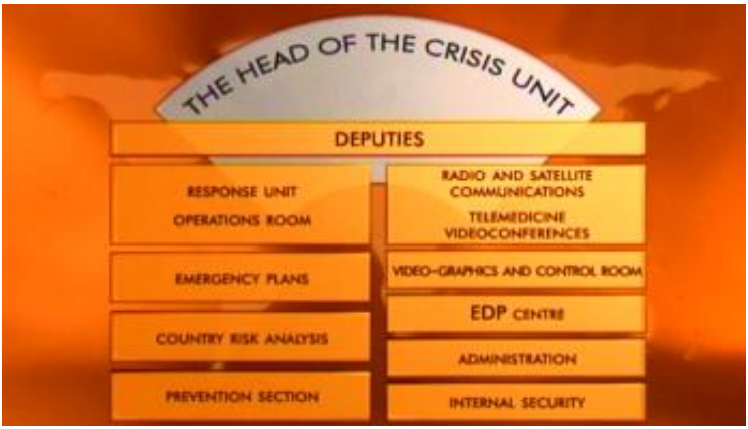


Рис. 7.8.

К особенностям СКЦ МИД Италии можно отнести следующие. Двуединый институциональный мандат СКЦ (рис. 7.9.) – это помощь и спасение итальянцев, а также национальных интересов в чрезвычайных ситуациях за рубежом.

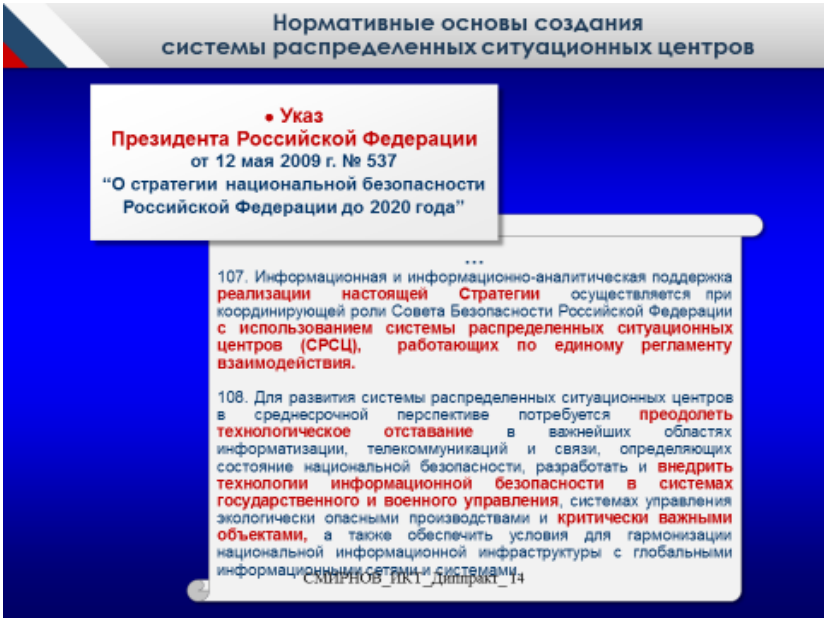
Рис. 7.9.

Мандат включает в себя компоненты (рис. 7.10.):

- 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.

Рис. 7.10.

7.4.4. Система ситуационных центров органов государственной власти России



Цель и основные задачи создания СРСЦ

ЦЕЛЬ СОЗДАНИЯ СРСЦ

Повышение эффективности государственного управления в мирное и военное время, а также при возникновении кризисных и/или чрезвычайных ситуаций на основе информационных и технологических возможностей ситуационных центров ОГВ РФ

ЗАДАЧИ СРСЦ

- Проведение скоординированных организационно-технологических мероприятий и согласованных действий по интеграции действующих СЦ в СРСЦ на основе единого регламента
- Создание новых и модернизация действующих СЦ с учетом перспективных типовых решений по составу программно-технических комплексов и защищенной информационно-телекоммуникационной инфраструктуры
- Формирование территориально распределенного государственного фонда, доступ к информационным ресурсам которого должен обеспечиваться на основе единого рубрикатора и с использованием технологий информационных порталов
- Разработка и внедрение информационных комплексов СРСЦ организация их взаимодействия с ведомственными и территориальными информационными комплексами
- Организация управления и координации взаимодействия в СРСЦ на основе единого регламента
- Обеспечение требуемого уровня информационной безопасности информационно-коммуникационной инфраструктуры СРСЦ
- Разработка нормативных документов, определяющих порядок создания, функционирования и развития СРСЦ
- Организация подготовки кадров для обеспечения функционирования СРСЦ, включая подготовку специалистов в области государственного стратегического прогнозирования, планирования и управления

31.03.2014

Состав и структура СРСЦ

- Комплексы программно-технических средств СЦ ОГВ

- Единый распределенный информационный фонд

- Комплексы информационных систем

- Защищенная телекоммуникационная сеть

- Комплекс информационной безопасности

- Центр управления и координации

31.03.2014

В настоящее время в России функционирует следующая система[246] взаимодействующих ситуационных центров органов госвласти, включающая в себя три уровня (рис. 7.11.):

Рис. 7.11.

Высший уровень - это ситуационный центр Президента России. Наряду с аналогичными комплексами президента США, правительств Германии и ряда других ведущих стран мира, он является одним из наиболее технически совершенных в мире. Работают ситуационные центры Администрации Президента и Правительства России. На втором уровне нахо-

[246] 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.

дятся ситуационные центры полномочных представителей Президента России в федеральных округах, руководителей министерств (Национальный центр управлениях в кризисных ситуациях (НЦУКС) МЧС России (рис. 7.12.), МИД России и т.д.), агентств (Росатом) и служб. На третьем уровне – ситуационные центры глав субъектов Российской Федерации и муниципальных образований[247].

Рис. 7.12. НЦУКС МЧС России

В успешной подготовке и проведении зимней Олимпиады 2014 важную роль сыграла специальная территориально-распределенная информационная система проектного управления (рис. 7.13.):

[247] 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.

Рис. 7.13.

7.4.4.1. Национальный центр управления обороной государства

В условиях резкого возрастания конфликтного потенциала в мире Указом **Президента России от 10 декабря 2013 г. создается Национальный центр управления обороной государства (НЦУОГ).**

Создаваемый центр станет основным звеном в системе управления военной организацией государства, связывающим действующие в России ведомственные (силового блока) системы управления и мониторинга.

В НЦУОГ, совместно с федеральными органами исполнительной власти, будут приниматься решения в области обороны, управления повседневной деятельностью Вооруженных Сил, других войск и воинских формирований, а также их всестороннего обеспечения.

Задача эксперта - предложить грамотное меню,
задача политика - не ошибиться в выборе блюд.
Василий Леонтьев

7.5. Информационно-аналитические системы (ИАС)

7.5.1. ИАС мониторинга и контент-анализа социальных сетей – опыт США

7.5.1.1. ИАС мониторинга и контент-анализа соцсетей в предвыборных кампаниях Б.Обамы

Рис. 7.14.

7.5.1.1.1. ИАС «Looking glass» Microsoft

В ходе кампании 2012 г. Б.Обама получил усовершенствованную ИАС (рис. 7.15.).

Рис. 7.15.

Компания Microsoft разработала инструмент для анализа социальных медиа (рис. 7.16.), который позволяет организациям быстрее реагировать на происходящее в социальных медиа и предпринимать соответствующие шаги.[248]

В случае увеличения активности в социальных медиа продукт присылает уведомление по электронной почте, в котором указывается направленность (негативная или позитивная) обсуждения и уровень влиятельности того, кто дал старт дискуссии. Кроме того, по диаграммам можно увидеть колебания активности на сервисах Twitter, Facebook, Flickr, YouTube и т.п. по дням.

Потоки данных из социальных медиа могут быть связаны с другими элементами бизнеса: базами данных клиентов, центров CRM, данными о продажах и т.д. Интеграция возможна при помощи продуктов Microsoft Outlook и Sharepoint.

[248] http://promarketing.by/looking-glass-produkt-microsoft-ot-dlya-monitoringa-socialnyx-media.html 20.06.2014

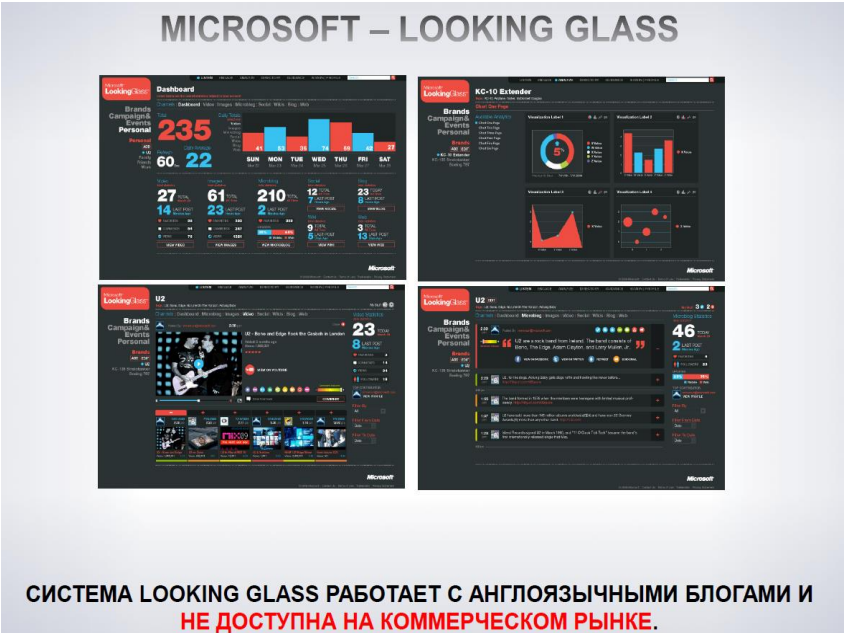


Рис. 7.16.

7.5.1.2. ФБР разрабатывает новую ИАС контент-анализа соцсетей

ФБР создает систему раннего предупреждения о различных угрозах на основе автоматического анализа информации из социальных сетей.

19 января 2012 г. Центр стратегической информации ФБР разместил на сайте запрос на создание «Приложения по социальным сетям».

В документе сказано: «Социальные сети стали основным источником разведывательной информации, так как в них можно найти первую реакцию на ключевые события».

Согласно объявлению, программа должна собирать информацию из «открытых источников» и иметь возможность:

- Обеспечить автоматизированный поиск и фильтрацию

информации из социальных сетей, включая Facebook и Twitter.

- Позволять поиск по новым ключевым словам.
- Отображать различные уровни угроз на картах, возможно, с использованием цветового кодирования для обозначения приоритетности угроз. Предпочтительно использование карт Google 3D и Yahoo Maps.
- Предусматривать широкий спектр данных о терроризме - как в США, так и во всем мире.
- Переводить твиты с иностранных языков на английский.

Характерно, что ФБР обратилось к подрядчикам через три недели после обнародования Советом по нацбезопасности США доклада о мониторинге соцсетей.

В документе также перечислены сайты, которые планирует отслеживать ФБР: YouTube, фотосервис Flickr, а также Itstrending.com - сайт, который показывает наиболее популярные записи на Facebook.

Указаны также ключевые слова. К ним относятся «банды», «оспа», «утечка», «вспомнить» и «2600» - цифра, журнала для хакеров.

Следует отметить, что Лондонская правозащитная организация Privacy International, заявила о беспокойстве последствиями такой деятельности ФБР.[249]

7.5.2. Основные отечественные ИАС мониторинга и анализа СМИ и соцсетей

В последнее время в России создано достаточно много ИАС мониторинга и анализа СМИ и соцсетей. Рассмотрим наиболее известные.

[249] http://www.bbc.co.uk/russian/international/2012/01/120127_fbi_social_networks.shtml

7.5.2.1. ИАС «Медиалогия»[250]

В основе продуктовой линейки компании лежит обширная база источников информации (рис. 7.17., 7.18.), позволяющая осуществлять мониторинг более 18 000 СМИ и более 92 млн. соцмедиа-ресурсов.

Глубина архива ряда источников превышает 10 лет.

Четкая структура позволяет с легкостью фильтровать источники информации по различным категориям и географии.

Оперативное поступление контента 24 часа в сутки, в том числе транскрипты федеральных телеканалов через 1,5 часа после выхода сюжета в эфир.

В системе доступны Первый канал, Россия 1, НТВ, РЕН ТВ, ТВ Центр, РБК ТВ, Пятый канал, Телеканал Дождь.

Пользователи системы также имеют доступ к максимально полным лентам основных информационных агентств: РИА Новости, ИТАР-ТАСС, ПРАЙМ.

[250] http://www.mlg.ru/solutions/4executives/prizma/ 20.06.2014

Рис. 7.17.

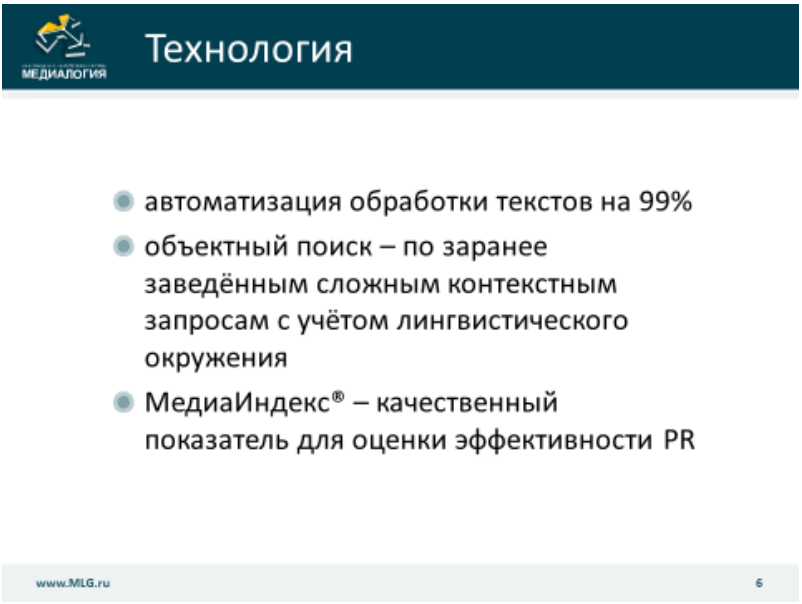


Рис. 7.18.

7.5.2.2. ИАС «ПРИЗМА»[251]

ИАС «ПРИЗМА» предназначена для руководителей федеральных и региональных органов государственной власти, это инструмент оперативного анализа социальных медиа для выявления резонансных проблем и рисков и, как следствие, своевременной реакции на них.

ИАС «ПРИЗМА» обеспечивает мгновенный мониторинг и оперативный анализ тональности высказываний и отношения населения к обсуждаемым проблемам, обрабатывает сообщения более 40 млн. русскоязычных соцмедиа: блогов, микроблогов, форумов и социальных сетей.

Возможности ИАС «ПРИЗМА»:

- анализирует интерес блогосферы к тем или иным проблемам и предупреждает о возможных репутационных рисках;
- позволяет оценивать реакцию в социальных медиа на основные события и инициативы ведомства, региона, руководителя;
- помогает отслеживать факты коррупции в рамках региона или ведомства и мгновенно реагировать на них;
- оперативно отслеживает в соцмедиа активности, приводящие к росту социальной напряжённости: нагнетание беспорядков, протестные настроения, экстремизм; обсуждение уровня цен, зарплат, пенсий; проблемы ЖКХ, инфраструктуры, медицины и др.;
- оперативно отслеживает электоральные настроения в соцмедиа по отношению к основным политическим партиям и их лидерам.

К ключевым особенностям данной ИАС относятся следующие:

- круглосуточный анализ настроений в социальных медиа и выявление аномального интереса к отдельным темам;

[251] http://www.mlg.ru/solutions/4executives/prizma/ 20.06.2014

- отслеживание тенденций в соцмедиа до попадания в СМИ;

- оперативность мониторинга - в режиме онлайн;

- оперативность анализа, недоступная при использовании других инструментов;

- настройка под задачи конкретного ведомства и руководителя.

ИАС «ПРИЗМА» обладает широкой областью применения: в кабинете руководителя; в предвыборном штабе; в ситуационном центре.

7.5.2.3. ИАС «Семантический архив 4.5»

ИАС «Семантический архив» представляет собой инструмент для создания интегрированного хранилища информации с возможностью хранения досье на объекты мониторинга, происходящие события, а также текстовые документы.[252]

Система позволяет хранить информацию, импортированную из различных реляционных баз данных, вводить информацию из любых других источников: Интернет, СМИ, баз данных, он-лайн библиотек и систем (Спарк, Интегрум и др.), любого документа, собственных сведений аналитика и пр. Это дает возможность объединять информацию, содержащуюся в различных документах и различных базах данных.

Гибко настраиваемая онтологическая модель данных позволяет работать с разными тематиками и сферами деятельности. Созданное хранилище служит аналитикам для поиска информации, добавления конфиденциальных собственных данных, выявления взаимосвязи между объектами и событиями, получения аналитических отчетов, схем, графиков и карт.

«Семантический архив» имеет модульную структуру, что позволяет легко подобрать и настроить нужную конфигура-

[252] http://www.anbr.ru/products/semarchive/ 20.06.2014

цию системы.

В новой версии упор делается на разработку платформы управления Интернет-роботами, отчетными формами, работе с графиками и геокартами, автоматизации выделения событий и фактов и ряде других новых функций.

Принцип работы ИАС «Семантический архив» представлен на рис. 7.19.

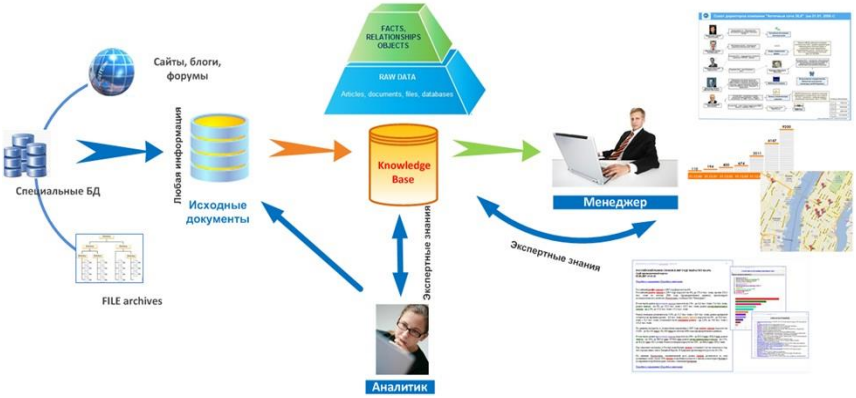


Рис. 7.19.

Возможности ИАС «Семантический архив»:

- Мониторинг и автоматический сбор информации из Интернет и других открытых источников (СМИ, аналитические отчеты, социальные сети, форумы, онлайн базы и др.);
- Объединения разнородных баз и банков данных в единую систему и поиск в ней информации по объектам интереса (персонам и организациям);
- Автоматическая обработка текстовых документов, выделение из них объектов интереса (персон, компаний, брендов и пр.) и связанных с ними фактов/событий;
- Полнотекстовый и объектный поиск, с помощью которого достигается высокая точность результатов;
- Быстрое выявление неявных (опосредованных) связей между объектами и связанными с ними фактами и событиями;

- Визуализация аналитических исследований в виде дайджестов, досье (бизнес-справок), семантических схем, графиков, геокарт и других видах отчетов.

Преимущества при внедрении системы заключаются в следующем:

- Автоматический мониторинг и поиск информации в Интернет.
- Документальное хранилище, в котором хранятся все важные статьи СМИ и внутренние документы компании. Система обеспечивает к ним мгновенный доступ с помощью функций поиска.
- Ведение досье по персонам, компаниям, регионам, крупным проектам, тендерам, ситуациям и пр. Факты из досье подтверждаются источниками (документами, статьями) в документальном хранилище.
- Визуальное описание ситуации любой сложности. Формирование многоуровневой и многоступенчатой картины развития ситуации. Все отношения между персонами и компаниями (партнеры, конкуренты, аффилированные структуры, заказчики, поставщики и т.п.) наглядно представлены на семантической сети.
- Разнообразные отчеты, карты, графики и дайджесты для руководства и менеджмента компании.

7.5.2.4. Комплекс обработки открытой информации ЗАО «Айкумен ИБС»

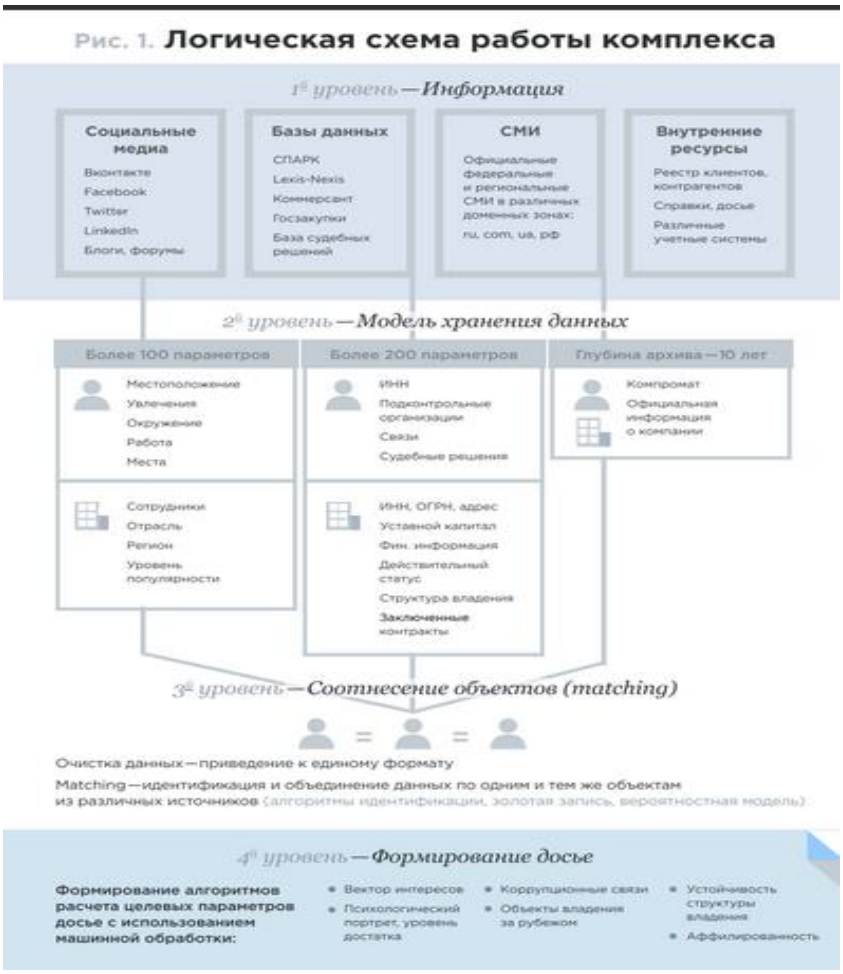


Рис. 7.20.

В процессе жизненного цикла любой объект, будь то персона или организация, оставляет в информационном пространстве след - информационный шлейф. Однако сбор этого шлейфа - лишь начальная стадия в процессе формирования

полноценного досье, которое должно быть заточено под решение определенных задач.

С точки зрения автоматизации процесса сбора досье возникают проблемы двух классов: на уровне данных и на уровне алгоритмов обработки данных.

Первый этап требует использования в Комплексе различных технологий сбора – от классических (запросы-ответы, использование функций API) до web-технологий, применяемых для получения данных из html страниц со сложными алгоритмами обхода страниц, регистрацией на ресурсах, защиты от блокирования и т.д.

Далее - нормализация и валидация данных. Для этого в Комплексе существуют алгоритмы нормализации данных. Описанный процесс играет ключевую роль, поскольку позволяет привести данные из разных по своей структуре и надежности ресурсов к единому виду. Данная подсистема совмещает в себе сложную ETL систему с огромным количеством коннекторов и web-роботов, а также модуль Data Quality.

Каждый ответ, полученный из источника, - официальные базы данных или профиль из соцсети - формирует в Комплексе свой объект: физическое или юридическое лицо. Естественно, что для комплексного анализа, необходимо иметь объединенные виртуальные образы одного и того физического объекта с целью формирования «золотой» записи – полного атрибутивного представления объекта. Для этой цели в Комплексе применяется конструктор идентификации объектов (matching object).

Пользователи вИинтернете редко указывают ИНН, но у них есть год и дата рождения, регион проживания, а также имя и фамилия, которые приводятся к каноническому виду с помощью справочников и сравниваются с официальными данными.

Другим интересным методом идентификации людей является «environment matching» - идентификация на основе окружения пользователя в соцсетях. Данные функции реали-

зуются во встроенной в Комплекс подсистеме MDM (Master Data Management).

Далее становится возможным проводить «ручное» исследование объекта.

Но, помимо затраченных временных ресурсов, возникает проблема глубины анализа данных. Например, построение графа связей аффилированности организации хотя бы до 3 уровня, приведет к появлению на диаграмме более 100 объектов (физических и юридических лиц), исследование каждого из которых займет массу времени.

Алгоритм построения цепочки связей исследуемого объекта с проблемными компаниями задается на программном уровне аналитиком и все, что необходимо сделать – выбрать этот кейс проверки из библиотеки кейсов. Аналогично автоматически рассчитывается вектор интересов персоны.

Данный подход позволяет максимально упростить процесс формирования «умного» досье на объект, а во-вторых, накопить библиотеку сценариев проверки, что является бесценным опытом.

Необходимым условием развития является внедрение новых технологий как в средствах сбора данных, так и в средствах их обработки. Так, для хранения и обработки больших массивов данных (более 10 млн. новых документов в сутки) в Комплексе применяются технологии Hadoop для распараллеливания вычисления на сотни кластеров. Для разбора текстов на естественных языках используются лингвистические модели для машинной обработки и т.д.

Продолжается совершенствование методов анализа данных, ведутся работы в построении модуля анализа целых групп персон и организаций как единого целого и т.д.

7.5.2.5. Веб-сервисы по глобальным техногенным, природогенным и иным чрезвычайным ситуациям

В последнее время появился ряд открытых веб-сервисов по глобальным техногенным, природогенным и иным чрезвычайным ситуациям.

Наиболее информативен и удобен в работе ресурс http://hisz.rsoe.hu/

Здесь можно найти в онлайне информацию по техногенным, природогенным и иным чрезвычайным ситуациям в мире и частям света (рис. 7.21., 7.22.).

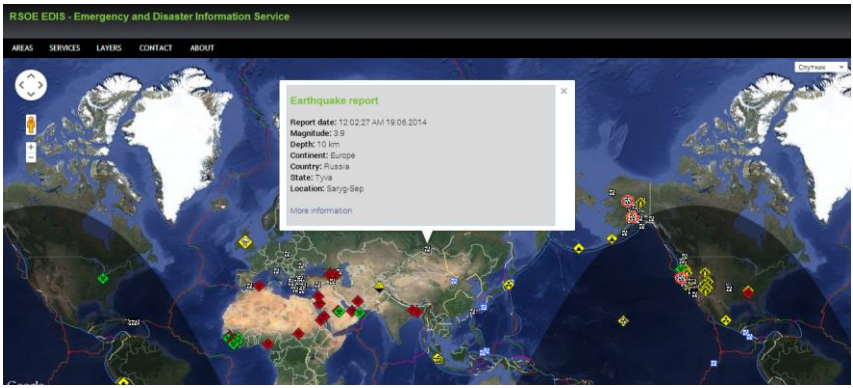


Рис. 7.21.

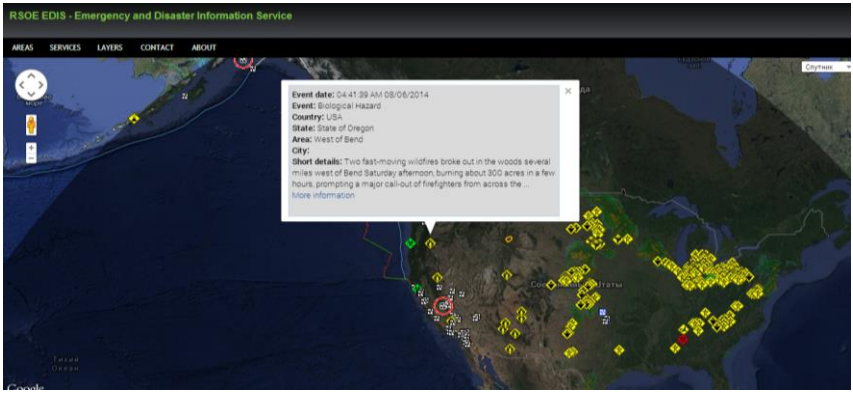


Рис. 7.22.

Полезен ресурс http://kosmosnimki.ru/, имеющий несколько информационных слоев: погода, пожары, многоаспектный поиск и т.д. (рис. 7.23.).

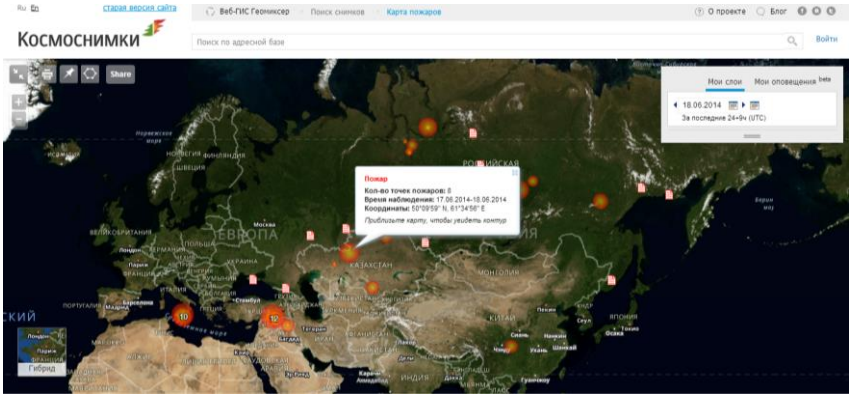


Рис. 7.23.

8. «МЯГКАЯ СИЛА» И ИНФОРМАЦИОННАЯ ДИПЛОМАТИЯ

8.1. Базовые теоретико-методологические подходы к фактору «мягкой силы»

Как уже отмечалось (гл. 4) фактор «мягкой силы» во многом изменил алгоритм международных отношений.

Большинство экспертов справедливо считают патриархом понятия «мягкая сила» Дж. Ная. Действительно, в 1990 году он ввел в политологический лексикон **термин «мягкая сила», который означает «способность одного государства к изменению поведения другого с помощью средств привлечения и убеждения»**[253].

Вместе с тем, главным разработчиком технологий политики ненасильственных действий является профессор Джин Шарп (1928 г.р.), основатель института Альберта Эйнштейна в Кэмбридже (1983 г.).

8.1.1. Работа Д.Шарпа «От диктатуры к демократии» - практическое пособие «цветным» революционерам

Наряду с трехтомным трудом Д.Шарпа «Политика ненасильственных действий», наибольший интерес представляет брошюра «От диктатуры к демократии. Концептуальные основы освобождения». Данная работа позиционируется сегодня как практическое пособие для оппозиции по ненасильственному свержению «диктаторских режимов». В силу этого ее содержание актуально не только «цветным революционерам», но и тем, кто их идеологии не разделяет.

[253] Nye, J., (2004), Soft Power: The means to success in world politics, New York, Public Affairs.

Д.Шарп длительное время изучал вопросы о том, как можно предотвратить или ликвидировать диктатуру. Данный интерес объясняется его убеждением о том, что человеческая личность не должна подавляться и уничтожаться подобными режимами (не без влияния работ о важности соблюдения прав человека и о природе диктатуры от Аристотеля до аналитиков тоталитаризма).

Представленные в работе Д.Шарпа общие принципы организации политического противостояния и реализации конкретных действий во многом универсальны, и они могут быть использованы как оппозицией, так и против нее.

В предисловии к Интернет-изданию своей книги Д.Шарп в октябре 1993 г. не скрывает того, что данный анализ станет стимулом для лидеров сопротивления при выработке стратегии, способной повысить его мощь и в то же время сократить сравнительный уровень потерь.

Труд Д.Шарпа отличается своей «технологичностью», т.е. минимумом идеологических маркеров, которыми страдают работы ряда современных «политтехнологов».

Если попытаться проанализировать все 198 методов, скрупулезно структурированных и описанных Д.Шарпом, то в них нетрудно увидеть арсенал «цветных» революций, прошедших в мире за последние четверть века, начиная от «методов ненасильственного протеста и убеждения» и кончая «мятежами» и государственными переворотами. Трагический пример Украины тому подтверждение.

Без знания изложенных методов невозможно понять алгоритма «цветных» революций, а, значит, осуществлять адекватные контрмеры и проводить эффективную превентивную контрпропагандистскую работу.

В силу этого, работа Д.Шарпа, как методическое пособие для оппозиционеров, рекомендуется к прочтению и изучению не только им, но и власть предержащим.

Д.Шарп 20 августа 2012 г. в ответе на вопрос о значении социальных сетей как факторе «цветных революций» под-

черкнул, что никакого принципиально нового вида протеста социальные сети не породили. «Забастовка может идти в Интернете, но она не перестает быть забастовкой. Дело в другом. Соцсети - это система оповещения, позволяющая в считанные минуты мобилизовать массы людей. Информация распространяется мгновенно, при этом отправителя идентифицировать нелегко. Это дает основу для расцвета провокаций, так как зачастую невозможно установить, кто является настоящим автором исходного сообщения с приглашением на митинг или призывом к какой-либо форме протеста. Подобные провокации опять же могут привести к тому, что мирный протест перерастет в насильственный, или же к тому, что люди придут не в то место, в которое их хотели позвать организаторы.

В эту эпоху протестующим необходимо быть очень умными и осторожными и, прежде чем присоединиться к какой-либо акции, внимательно разобраться, кто на самом деле распространяет о ней сообщения.»[254]

8.1.2. «Мягкая сила» по Джозефу Наю

Анализ работ отечественных и зарубежных авторов по проблематике «мягкой силы», которую ряд экспертов уже возвели в ранг доктрины, показывает, что ее несомненным патриархом является американский политолог Джозеф Най.

В предисловии к статье Дж.Ная «Soft power, или «мягкая сила» государства», опубликованной в декабре 2006 г. в № 5 (41) альманаха «Восток» отмечается, что на пороге XX века США пришли к выводу о безопасности не только в Западном полушарии («доктрина Монро»), но и на евразийском континенте - особенно на западной и восточной его оконечностях. В силу этого понятно вторжение США в топливную кладовую мира – Ближний Восток и прилегающие регионы.

[254] http://www.gazeta.ru/politics/2012/08/20_a_4731409.shtml

США за последние 70 лет создали два «мирных» фактора своей мощи: господство над международной валютной системой и систему свободной торговли.

Однако особую роль сыграл третий - привлекательность, или «soft power» - «мягкая сила». Действительно, ученые всего мира считают США кузницей нобелевских лауреатов, женщины - оплотом феминизма, болельщики поклоняются американскому спорту, киноманы - Голливуду, дети - Диснейленду, интернетчики - родине Интернета и глобальных социальных сетей.

Термин «soft power» или «smart power» - «мягкая сила» (имеются и иные варианты перевода) вот уже несколько лет в топ-листе тем научно-экспертных и политико-дипломатических кругов. При этом Евросоюз отдает предпочтение переводу термина как «собранная, скоординированная сила», Китай - как «мудрая сила» (отражает суть китайской дипломатии, ее конфуцианские корни стратегической культуры и стратагем).

Для небольших государств «мягкая сила» - это синоним эффективности соотношения ограниченных ресурсов влияния и дипломатического успеха, а также инновационности, экологичности и т.д.

Итак, термин «soft power» выступает своего рода прикрытием разнообразных толкований, и это обусловливает его популярность. Так, Дж.Най, введя его в предвыборные дискуссии в США, оказался убедительным и для республиканцев, и демократов.

Дж.Най, понимал под властью способность добиваться желаемых результатов следующими тремя путями: принуждение, подкуп и привлекательность. Два первых подпадают под понятие жесткой власти, в то время как привлекательность - это признак мягкой власти.

Следует особо подчеркнуть, что, вводя термин «мягкая сила», Дж.Най указывал на недостаточность использования одного из этих двух базовых ресурсов отдельно от другого.

Дж.Най продолжает свои исследования. В своей статье в апреле 2012 г. «Кибервойна и мир» он касается особо чувствительной - военно-политической составляющей международной информационной безопасности - информационных войн как войн шестого поколения (подробнее см. в 4.4).

Дефиниция «мягкая сила» была конкретизирована и уточнена с учетом современных реалий, а, учитывая стремительное развитие ИКТ, подтверждена его эффективность как инструмента для достижения политических целей государства. Многие аналитики отмечают, что 2010 год является важной вехой для развития фактора «мягкой силы, т.к. именно этот период стал переходным от дебатов к количественному и качественному измерению данного фактора[255].

8.2. Рейтинг фактора «мягкой силы» в ведущих странах мира

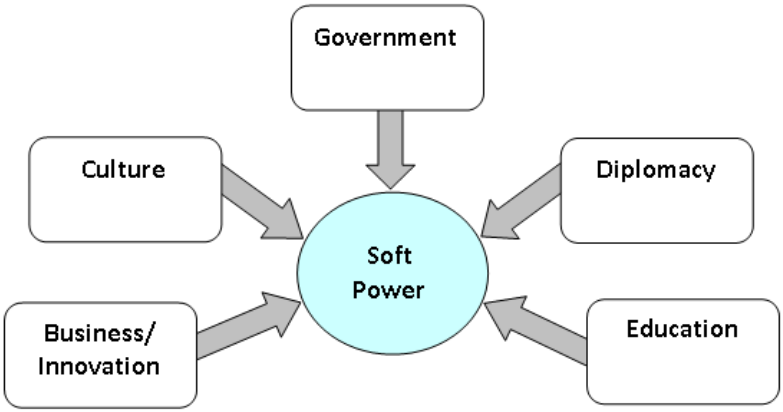
Для изучения степени использования фактора «мягкой силы» во внешней политике различных государств представляется оправданным проанализировать подготовленный в 2013 г. **английским независимым Институтом управления и аналитическим журналом «Монокль» международный рейтинг фактора «мягкой силы» (A 2013 Global Ranking of Soft Power)**.

Английский независимый Институт управления и аналитический журнал «Монокль» впервые опубликовали данный рейтинг четыре года назад, используя широкий набор статистических и субъективных показателей, распределенных по пяти категориям. Причем три из них, по мнению Дж.Ная, являются основными критериями, отражающими фактор «мягкой силы» государства, - это **культура, политические цен-**

[255] The New Persuaders III. A 2012 Global Ranking of Soft Power

ности и внешняя политика[256]. Авторы рассматриваемого рейтинга, как и в предыдущие годы, опираются на расширенный список данных факторов, которые включают в себя также категории **«Бизнес/Инновации»** и **«Образование»** (см. схему 8.1.)[257].

Схема 8.1.



В силу того, что единой методики для измерения фактора «мягкой силы» не существует, при составлении данного рейтинга авторы опирались на ряд международных исследований, позволяющих оценить позицию страны по каждому из пяти факторов. Среди используемых данных -исследования ООН, ОЭСР, ЮНЕСКО, Мирового Банка, а также Индекс Анхольта[258] (Anholt-GFK Nation Brand Index 2013), Индекс глобальной конкурентоспособности 2013-2014 (Global Competitiveness Report 2013-14, World Economic Forum)[259], Международный индекс транспарентности (Transparency International Corruption Perception Index), Индекс визовой до-

[256] Nye, J. (2004) Soft Power: The means to success in world politics, New Your: Public Affairs
[257] См. http://www.instituteforgovernment.org.uk/publications/new-persuaders-ii 19.06.2014
[258] http://www.gfk.com/news-and-events/press-room/press-releases/pages/nation-brand-index-2013-latest-findings.aspx 19.06.2014
[259] http://www.weforum.org/reports/global-competitiveness-report-2013-2014 19.06.2014

ступности стран[260] (The Henley Visa Restrictions Index 2013), присутствие страны в сети Интернет и др.

8.2.1. Критерии составляющих «мягкой силы»

Для лучшего понимания рейтинга представляется оправданным конкретизировать, какие именно показатели «мягкой силы» использованы для каждого критерия:

«Культура» - количество туристов, посещающих страну ежегодно, использование языка страны в мире, количество памятников Всемирного наследия ЮНЕСКО, успех страны в Олимпийских играх, влияние культурного наследия страны на мировую культуру в целом.

«Политические ценности» - критерий измеряет привлекательность политических ценностей, эффективность деятельности политических институтов государства, модель национального правительства: прозрачность, демократичность и др. Однако, как отмечают сами авторы исследования, индекс политической привлекательности страны смещен в сторону западных политических концепций.

«Дипломатия» - способность страны формировать благоприятный образ для мирового сообщества, внешняя политика и дипломатические ресурсы, членство в международных организациях и наличие культурных миссий за рубежом и др.

«Образование» - количество иностранных студентов в стране, качество высшего образования, наличие программ обмена студентами, количество учебной литературы и др.

«**Бизнес / Инновации»** - привлекательность экономической модели страны: открытость, способность к инновациям, уровень коррупции, конкурентоспособность отраслей экономики, регулирование.

С учетом того, что данный международный рейтинг фактора «мягкой силы» составляется уже в четвертый раз, его

[260] https://www.henleyglobal.com/index.php?id=10 19.06.2014

разработчики внесли некоторые качественные изменения для получения наиболее точных данных.

В частности, одним из важных изменений, без которого было бы невозможно в полной мере определить влияние «мягкой силы» государства, явился «цифровой» индикатор: проанализированы данные о количестве подписчиков на Twitter-аккаунты министерств иностранных дел и министров иностранных дел исследуемых стран. В критерий «Культура» были добавлены 2 новых показателя: проникновение музыки государства на глобальные рынки, данные Международной федерации фотоиндустрии (International Federation of Phonographic Industry) для определения страны происхождения для наиболее продаваемых художников и данные о киноиндустрии.

По итогам проведенных расчетов, Рейтинг использования фактора «мягкой силы» представлен в Таблице 8.1.

8.2.2 Анализ рейтинга использования фактора «мягкой силы» по странам

Международный рейтинг фактора «мягкой силы» (A 2013 Global Ranking of Soft Power) проводился среди 30 стран, в настоящем исследовании приведем лишь топ-10.

Таблица 8.1.

Рейтинг использования фактора «мягкой силы» по странам[261]

Место 2013	Страна	Место 2012
1	**Германия**	3
2	**Великобритания**	1

[261] http://monocle.com/film/affairs/soft-power-survey-2013/

Место 2013	Страна	Место 2012
3	**США**	2
4	**Франция**	4
5	**Япония**	6
6	**Швеция**	5
7	**Австралия**	9
8	**Швейцария**	8
9	**Канада**	10
10	**Италия**	14

В 2013 году в топ-10 стран данного рейтинга присутствуют те же государства, что и в подобном рейтинге 2012 г., изменились лишь их позиции в рейтинге, и только Италия вытеснила Данию из первой десятки и переместилась с 14 на 10 место.

Возглавила рейтинг **Германия**. По мнению авторов, на повышение рейтинга оказало влияние усиление позиций Германии в Европе в последние годы благодаря деятельности правительства, возглавляемого А.Меркель, а также непререкаемая репутация немецких брендов, культуры и спорта. При этом отмечено, что ФРГ традиционно вкладывает огромные бюджетные средства в публичную дипломатию, в т.ч. на обеспечение деятельности Международной телерадиокомпании ФРГ «Deutsche Welle»; Института им.Гете, насчитывающего 172 миссии в различных странах, проводя работу по продвижению немецкого языка и культуры за рубежом. Правительство Германии также осуществляет мероприятия по увеличению количества иностранных студентов среди общества числа студентов ФРГ.

Лидер рейтинга 2012 года – **Великобритания –** заняла 2-е место. Помимо традиционного культурного наследия, исторических связей со многими странами, в т.ч. и с бывшими колониями, членства в различных международных организациях на позицию Великобритании в рейтинге огромное влияние

оказало проведение в Лондоне летних Олимпийских игр 2012 (что и позволило Великобритании возглавить рейтинг «мягкой силы» в год проведения Олимпийских игр в Лондоне).

США опустились на 3-е место. Понижение рейтинга США по сравнению с предыдущими годами эксперты связывают, прежде всего, с бюджетным кризисом внутри страны, а также участием США в обострении ситуации на Ближнем Востоке, в частности в Египте и Сирии, в Афганистане и Ираке, что негативно влияет на восприятие Америки в мире. При этом была дана высокая оценка культурной составляющей «мягкой силы» США, а также качеству высшего образования, привлекающему иностранных студентов.

Франция и Япония замыкают первую пятерку, имея в своем арсенале «мягкой силы» значительное количество дипломатических представительств в зарубежных странах, культурных миссий и объектов Всемирного наследия ЮНЕСКО.

Сингапур, Китай и Россия улучшили свои позиции в данном рейтинге по сравнению с 2012 годом, заняв соответственно 17, 20 и 27 места[262].

8.2.3. Особенности «мягкой силы» Китая

Анализируя результаты рейтинга, а также подходы государств к использованию фактора «мягкой силы» возникает вопрос, продолжает ли оставаться гегемоном в мире «мягкая сила» Запада?

Так, согласно полученным результатам, для **Китая** основным преимуществом «мягкой силы» являются культура и образование. За последние несколько лет Китаем создано 323 Института Конфуция, деятельность которых направлена на изучение китайского языка и культуры. В то же время гостелерадиокомпания КНР CCTV завоевывает англоязычную

[262] http://jpewinfield.wordpress.com/2014/01/14/methods-and-champions-of-soft-power/ 19.06.2014

аудиторию, открывая новые телестудии в США (Вашингтон), Западной Европе и Кении (Найроби)[263].

При этом в привлекательности КНР авторы исследования отмечают такие минусы, как цензура СМИ, неприятие критики политической системы, ограничение свободы личности.

В основе китайской стратегии «мягкой силы» лежит концепция «гармоничного мира». Новые политические инициативы, такие как «улыбчивая дипломатия», «публичная дипломатия» и «добрососедская дипломатия», играют важную роль в стремлении Пекина влиться в интеграционные процессы и стать неформальным региональным лидером.

Китайское определение «мягкой силы» шире западного, что открывает новые возможности ее применения. Китайские теоретики нередко цитируют образец древней мудрости, гласящий, что «в Поднебесной самое мягкое одерживает верх над самым твердым»[264].

Оно затрагивает две проблемы - укрепление глобальной притягательности Китая и нейтрализацию негативного влияния западной культуры на граждан КНР.

Согласно трактовке руководителя Института международных проблем университета Цинхуа Янь Сюэтуна**, комплексная сила страны сочетает в себе «жесткую» и «мягкую силу» не как сумма, а как произведение двух компонентов.**[265] Соответственно, при утрате «мягкой» или «жесткой силы» совокупная национальная мощь становится равной нулю (это перекликается с подходом Джозефа Ная о том, что одна сила не может работать без другой).

Сильной стороной китайского подхода к «мягкой силе» является ее принципиальная ненавязчивость, невмешательство в чужие дела, уважение к чужому суверенитету и самобытности, желание создать гармоничный справедливый ми-

[263] См. http://www.instituteforgovernment.org.uk/publications/new-persuaders-ii 20.06.2014
[264] К.И.Косачев. Не рыбу, а удочку. http://www.globalaffairs.ru/number/Ne-rybu-a-udochku-15642
[265] Там же.

ропорядок, который бы не ущемлял ничьих интересов и способствовал развитию каждого через равномерное развитие всех. Таким образом, можно сказать, что китайская версия «мягкой силы» адресована к довольным, а западная - к недовольным.

Анализ показывает, что масштабное инвестирование Китаем в выигрышные для него инструменты «мягкой силы» может предвещать начало **переломного момента в смещении центра использования фактора «мягкой силы» нового поколения с Запада на Восток**.

В то время как на Западе сокращают государственное финансирование ключевых традиционных институтов «мягкой силы» совершенно противоположный процесс происходит в странах Востока, активно инвестирующих в «мягкую силу нового поколения - 2.0».

8.2.4. Социальные сети как инструмент «мягкой силы 2.0»

В январе 2014 г. глобальные социальные сети охватили уже более 2 млрд. людей.

Соцсети – это база для краудсорсинга. Краудсорсинг основан на законе Джоя: в любой сфере деятельности больше знаний находится за пределами любой действующей в этой сфере структуры. Одновременно соцсети подтверждают «парадокс Нейсбитта»: чем сильнее процессы глобализации, тем сильнее роль ее единиц (рассмотренные ранее примеры Э.Сноудена, М.Найема и др. подтверждают данный парадокс).

В силу вышеизложенного стратегическое значение фактора «мягкой силы 2.0» по сравнению с «жесткой силой» будет возрастать, что уже учитывают концептуальные и доктринальные стратагемы внешней политики ведущих стран мира.

8.3. Дипломатия 2.0 – зарубежный опыт

Стремительное распространение новейших ИКТ не обошло и внешнеполитический инструментарий.

«Электронная дипломатия» (инновационная, цифровая, отрытая и т.д.) органично имплементируется в традиционную, классическую дипломатию.

Электронная дипломатия имеет обширный функционал[266]: популяризация политики того или иного государства, вовлечение в политические процессы как можно большего числа активных граждан за рубежом, создание положительного образа своей страны, повышение её репутации («гудвилла»), создание «союзов друзей», «фан-клубов», страноведение, дистанционное изучение языков, оповещение своих граждан в случае ЧП, прямая связь с местом катастрофы, привлечение иностранных интеллектуальных ресурсов для коллективного решения назревших проблем или возникших ситуаций.

[266] Болгов Р.В. «Политическое значение технологий Web 2.0 (на примере деятельности интернет-сообществ). В книге «Негосударственные участники мировой политики: учебное пособие для вузов. Под ред. М.М. Лебедевой и М.В. Харкевича». – М.: «Аспект Пресс», 2013.

Кроме того, электронная дипломатия - это:

- средство обратной связи, позволяющее дипслужбам прислушиваться к мнению «людей с улицы» (listening) и на этой основе проводить анализ общественного мнения или оценку качества своих действий и распространяемой информации о стране и её гражданах;

- канал «службы спасения» для сограждан в случае возникновения где-либо природогенных и техногенных катастроф и т.п.;

- средство проведения краткосрочных политических кампаний, направленных на продвижение конкретной политической идеи, действия и т.п. (advocacy);

- средство налаживания связей между диаспорами своих граждан, по тем или иным причинам проживающих за рубежом.

Таким образом, электронная дипломатия, с одной стороны, - способ продвижения внешнеполитических интересов государства в стране пребывания с использованием новейших ИКТ, а с другой - способ использования когнитивных технологий, для оказания влияния на процессы принятия решений человеком и его структуру рассуждений, когда объект воздействия считает, что он сам принимает решения, на самом же деле оказывается скрытно ведомым другими (рис. 8.1.).

Рис. 8.1.

8.3.1. Анализ рейтинга AFP «E-Diplomacy»

Для мониторинга продвижения внешнеполитических взглядов и влияния на общественное мнение деятельности государств путем использования ИКТ французским агентством AFP был впервые составлен рейтинг эффективности стран в сфере Интернет-сервисов eDiplomacy[267].

При этом учитывалась активность дипломатических ведомств в сети Интернет, прежде всего в социальных сетях, количество подписчиков на их аккаунты и цитируемость.

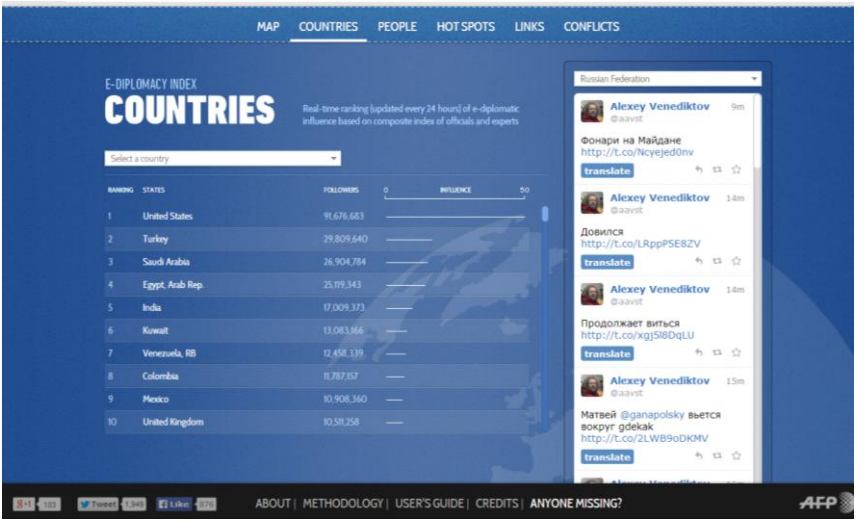
На сайте АФП[268] в режиме реального времени визуализируется, анализируется и измеряется глобальное присутствие и влияние в Twitter. По мнению экспертов, Twitter – один из эффективных инструментов электронной дипломатии, позволяющих государству увеличивать свое присутствие и влияние в сети Интернет, предоставлять объективную информацию зарубежной и отечественной аудитории.

Сердцем сайта является база данных, состоящая из более чем 6000 Twitter-аккаунтов, отражающих информацию о том, who's who в глобальной цифровой дипломатии: международные организации, государства, дипломатические ведомства, персоналии. Все расчеты, сделанные для формирования рейтинга основаны на этой базе данных. Постоянно обновляющиеся рейтинги стран и персон, а также инновационный интерфейс, по мнению создателей сайта, дают возможность пользователю наблюдать дипломатию «в действии».

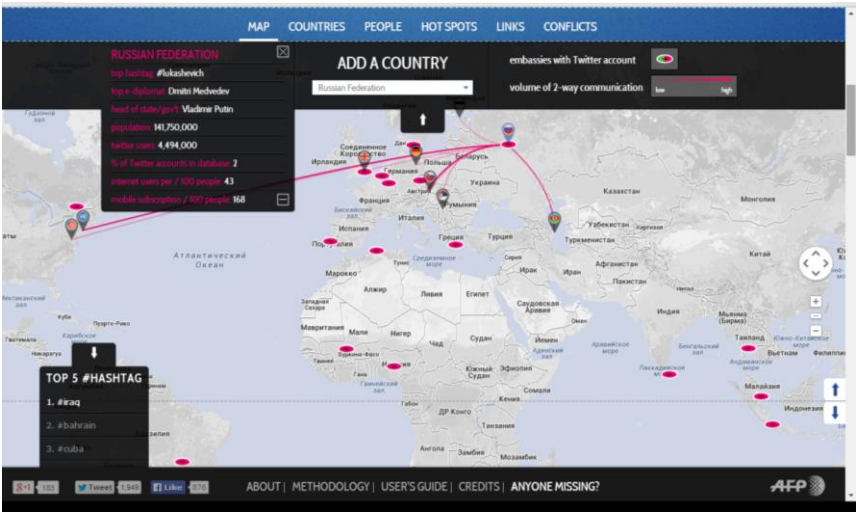
Так, по данным на 21 июня 2014 г., на первом месте из 152 стран находятся США[269]. На их аккаунты подписано более 91 млн. человек. В первой десятке рейтинга также Турция, Саудовская Аравия, Египет, Индия, Кувейт, Венесуэла, Мексика и Великобритания.

---

[267] http://ediplomacy.afp.com/#!/map
[268] http://ediplomacy.afp.com/
[269] http://ediplomacy.afp.com/#!/countries 21.06.2014



Россия в настоящее время занимает 13-е место[270]. Блоги россиян (в рейтинге учитывались и аккаунты первых лиц государства) читает более 7,3 млн. подписчиков.



[270] http://ediplomacy.afp.com/#!/countries 21.06.2014

Следует отметить, что в МИД России, в отличие от Госдепа США и дипведомств ряда других стран, **этой работой стали заниматься относительно недавно:**

- растущей популярностью пользуются открытые в июне 2011 г. официальные аккаунты МИД России на сервисе микроблогов «Twitter» (более 285 тыс.[271] подписчиков у русскоязычной и около 50 тыс.[272] - у англоязычной версии). Российскими загранучреждениями зарегистрировано более 130[273] учетных записей;

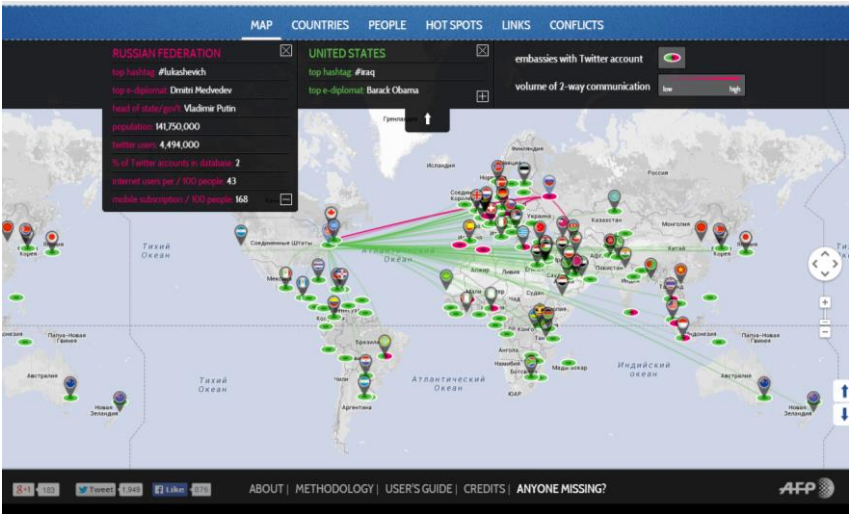
- летом 2012 г. в МИД России запущен официальный канал в YouTube[274];

- 21 февраля 2013 г. создан аккаунт МИД России в Facebook[275], где размещены актуальные и архивные материалы по российской внешней политике, информация российских загранучреждений, Россотрудничества, Фонда поддержки публичной дипломатии им А.М.Горчакова, Дипломатической академии, МГИМО(У), а также издания по тематике международных отношений и др.

8.3.1.1. США

Как было отмечено выше, США возглавляют рейтинг[276] АФП «**eDiplomacy**».

[271] https://twitter.com/MID_RF 21.06.2014
[272] https://twitter.com/MFA_Russia 21.06.2014
[273] http://www.mid.ru/bdomp/ministry.nsf/info/60B74D7F0544334044257A160028D471 21.06.2014
[274] http://www.youtube.com/user/midrftube 21.06.2014
[275] https://www.facebook.com/MIDRussia 21.06.2014
[276] http://ediplomacy.afp.com/#!/map 21.06.2014



Такое положение в рейтинге связано в том числе и с тем, что еще в 2003 году в Госдепартаменте США[277] была создана амбициозная глобально распределенная информационная система, которая, по сути, поставлена в центр всех информсистем госорганов США (рис. 8.2.).

[277] См. А.И.Смирнов. Информационная глобализация и Россия: вызовы и возможности. М.: Парад. 2005

Рис. 8.2.

В сентябре 2010 г. Госдепом США был разработан «Стратегический план развития информационных технологий в 2011–2013 гг.: цифровая дипломатия».[278] В данном плане, как и в тактическом плане **одним из ключевых инструментов в дипломатической практике правительства США было названо применение социальных сетей.** Реализация каждой внешнеполитической цели подкрепляется инструментами цифровой дипломатии, разработанными специалистами Офиса электронной дипломатии Госдепартамента США.

Американскими экспертами было предложено несколько концепций, описывающих специфику новых условий ведения цифровой дипломатии, или как ее еще называют «электронной дипломатии» как одного из наиболее актуальных методов

[278] IT Strategic Plan: Fiscal Years 2011-2013-Digital Diplomacy. Department of State. 01.09. 2010 http://www.state.gov/m/irm/rls/148572.htm. 20.06.2014

использования глобальной сети и ИКТ для осуществления внешнеполитической деятельности.

8.3.1.1.1. Основные составляющие цифровой дипломатии США

В стратегическом плане Госдепа выделено 8 тематических категорий электронной дипломатии[279]:

1) **Управление знаниями** (knowledge management): эффективное и оптимальное использование накопленных знаний, в т.ч. с целью защиты национальных интересов государства за рубежом.

2) **Публичная дипломатия** (public diplomacy): основная функция - поддержание контактов с целевой аудиторией посредством Интернет, с использованием новейших средств коммуникации для передачи важнейших сообщений и воздействия на целевую аудиторию в режиме реального времени.

3) **Управление информацией** (information management): использование соответствующей информации при принятии политических решений, а также для выработки превентивных мер для предупреждения новых вызовов и угроз.

4) **Консульское реагирование** (consular communications and response): создание специальных порталов для осуществления коммуникаций с гражданами, находящимися за рубежом, в т.ч. оказание содействия при возникновении кризисных ситуаций.

5) **Реагирование при возникновении чрезвычайных ситуаций** (disaster response)**:** использование возможностей ИКТ для реагирования в случае возникновения стихийных бедствий или иных чрезвычайных ситуаций.

6) **Обеспечение свободы сети Интернет:** создание технологий для поддержания открытости сети Интернет.

[279] http://e-gov.by/themes/best-practices/osnovy-ediplomacy-chast-1 20.06.2014

7) **Внешние ресурсы** (external resources)**:** использование специальных ИКТ для работы с зарубежными экспертами с целью продвижения своих национальных интересов.

8) **Стратегическое планирование** (policy planning): создание специальных технологий для обеспечения координации, планирования и эффективного контроля деятельности органов правительства в сфере международной политики.

Идея создания электронной дипломатии возникла в США еще в 2002 г. с учреждения целевой рабочей группы по проблемам электронной дипломатии (в настоящее время - Офис электронной дипломатии).

Сейчас в различных структурах Госдепартамента функционируют 25 узловых отделений электронной дипломатии. Некоторые из них фокусируются исключительно на проблемах, имеющих отношение к электронной дипломатии. Другие были учреждены на традиционных рабочих местах, например, в территориальных подразделениях, с целью облегчения адаптации к меняющимся условиям ведения дипломатии.

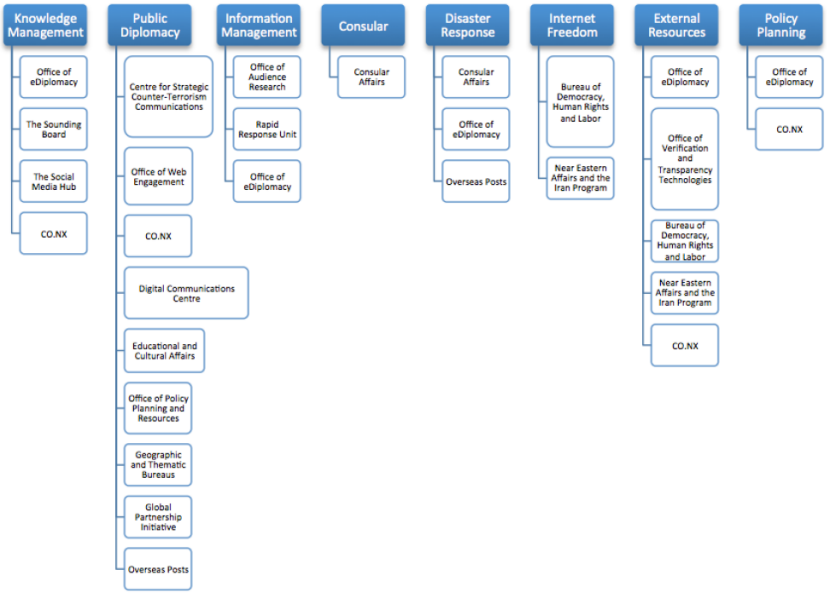
Система электронной дипломатии США включает в себя:

- 25 различных проектов, разработка которых ведется Госдепартаментом США в сотрудничестве с НПО и IT-компаниями;
- около 150 штатных сотрудников, часть из которых прикомандированы к другим подразделениям Госдепартамента;
- возможность использования электронной дипломатии сотрудниками американских посольств в различных странах мира.

8.3.1.1.2. Подразделения Офиса электронной дипломатии в общей структуре Госдепа США

Схема 8.2.

Подразделения Офиса электронной дипломатии в зависимости от реализуемых целей[280]



Офис электронной дипломатии стал ключевым решением для управления знаниями в Госдепартаменте США. Его миссия - совершенствование дипломатии благодаря развитию эффективных инициатив по обмену знаниями, разработке правил по взаимодействию между технологиями и дипломатией, а также первоклассному консалтингу в области информационных технологий[281].

[280] См. www.lowyinstitute.org/publications/revolutionstate-spread-ediplomasy
[281] http://www.state.gov/m/irm/ediplomacy/

В рамках стратегии по управлению знаниями (утверждена Госдепом США в августе 2003 г.) в Офисе электронной дипломатии был разработан соответствующий инструментарий, позволяющий решать следующие задачи в рамках электронной дипломатии:

- использовать онлайн-сообщества для обмена знаниями;
- оптимизировать способы поиска информации для более эффективного ее использования;
- совершенствовать методы обмена опытом и экспертными оценками с коллегами;
- использовать технологии, позволяющие максимально упростить обмен знаниями, с тем, чтобы он стал частью повседневного рабочего процесса.

Среди основных проектов Офиса электронной дипломатии Госдепа США можно выделить следующие.

8.3.1.1.3. Электронная энциклопедия американской дипломатии Diplopedia

Diplopedia разработана в 2006 г. и представляет собой вариант Wikipedia для внутреннего использования (дизайн и концепция Wiki сохранены для удобства пользователей).

Рис. 8.3. Главная страница Электронной энциклопедии американской дипломатии **Diplopedia**[282]

[282] См. http://www.state.gov/m/irm/ediplomacy/115847.htm 20.06.2014

Платформа также использует бесплатное программное обеспечение MediaWiki. В октябре 2012 г. платформа насчитывала уже свыше 20 тыс. статей, а также более 5 тыс. зарегистрированных пользователей. Зафиксировано около 100 тыс. просмотров страниц энциклопедии, а также сотни тыс. редакций различных статей: от списка кандидатов на повышение (Promotion List) до информационных заметок посольства США в Хартуме (Embassy Khartoum Portal).[283]

В настоящее время Diplopedia представляет собой:

- центральное хранилище информации Госдепартамента США, что особенно важно при работе с редко встречающейся или незнакомой проблематикой;
- центр обмена знаниями и инструмент их распространения. Примером является Deskipedia - страница с практической информацией и полезными ссылками для новых референтов;
- пространство для создания отчетов. Например, сотрудник, работающий в Вашингтоне, получил задание создать отчет о специфике участия граждан в религиозных организациях в различных странах мира. Создав страницу в Diplopedia, пользователь имеет возможность обратиться к сотрудникам о размещении отчетов по своим странам прямо на странице. Затем на основании анализа полученных данных составляется искомый отчет.

8.3.1.1.4. Система тематических сообществ Communities@State blogs

Система тематических сообществ Communities@State blogs[284] учреждена в 2005 г., представляет собой более 70 тематических сообществ блогеров и насчитывает 46 500 посетителей, которыми оставлены 5 600 комментариев по широ-

[283] Там же.
[284] См. www.lowyinstitute.org/publications/revolutionstate-spread-ediplomasy

кому кругу вопросов: от стратегии и управления до языков и социальных интересов.

Сообщества и блоги предлагают следующие возможности:

- наладить сотрудничество между ведомствами и отделами по любой проблематике, будь то засекреченная либо открытая тема с наименьшими временными затратами;

- осуществлять консультации коллег посредством общения в сообществах;

- осуществлять обмен знаниями по широкому кругу вопросов;

- вести текущие дела путем создания специализированного блога.

В отличие от специализированной сети Corridor, система тематических сообществ Communities@State позволяет вести развернутые дискуссии среди пользователей. Все записи архивируются и индексируются, их легко найти через правительственный поиск.

8.3.1.1.5. Профессиональная служебная сеть американских дипломатов Corridor

В 2011 г. была запущена **профессиональная служебная сеть американских дипломатов Corridor**[285]. Для удобства пользователей дизайн и общий механизм функционирования Corridor был преднамеренно выполнен в стиле социальной сети Facebook.

На октябрь 2011 г. в сети Corridor было зарегистрировано 6 800 пользователей (800 активных) и более 440 групп[286].

В отличие от Facebook, вся информация на Corridor доступна всем государственным служащим, здесь нет личных сообщений и возможности скрыть информацию в профиле. Среди основных возможностей сети Corridor можно выделить следующие:

---

[285] http://www.state.gov/m/irm/ediplomacy/c23840.htm 21/06/2014

[286] См. www.lowyinstitute.org/publications/revolutionstate-spread-ediplomasy

- Группы. Пользователю доступно размещение протоколов совещаний, составление графика мероприятий, опубликование отчетов сотрудников;

- Поиск коллег с определенным набором профессиональных качеств;

- Обмен мгновенными сообщениями;

- Обмен знаниями и информацией, в т.ч. размещение ссылок, как на внутренние документы, так и на внешние ресурсы.

В проекте есть опция размещения стандартной биографической информации о сотрудниках на Corridor самими пользователями, что способствует, в т.ч. повышению качества работы кадровой службы Госдепа США: своевременное обновление баз данных, поиск подходящих сотрудников на вакантные должности и пр.

8.3.1.1.6. Virtual Student Foreign Service

Виртуальный студенческий сервис по международной проблематике (Virtual Student Foreign Service[287]) был запущен в 2009 г. по инициативе госсекретаря США Х.Клинтон[288]. Данный сервис призван знакомить американскую молодежь с деятельностью дипломатических миссий США.

Для осуществления данных целей используются следующие методы:

- осуществляется пиар-кампания с использованием социальных сетей таких, как Facebook, Twitter, MySpace, YouTube и т.д.,

- размещение графической и иной информации на сайтах дипмиссий США по широкому кругу вопросов;

[287] http://www.state.gov/vsfs/209292.htm 21.06.2014

[288] «The First Quadrennial Diplomacy and Development Review». The United States Department of State. Retrieved 2 April 2012.

- размещение статей на страницах дипмиссий США в Facebook по проблематике Интернета, ИТ-технологий, истории и литературе.

В рамках программы электронной дипломатии **Tech@State** создаются технологические решения для повышения качества образования, здравоохранения и других сфер жизнедеятельности.

Программа **TechCamps** включает в себя ряд учебных мероприятий в разных городах мира для технологической поддержки запущенного в 2010 г. по инициативе Х.Клинтон проекта Civil Society 2.0[289]. Данный проект предполагает сотрудничество и обучение ведущими специалистами в области ИКТ с представителями НПО, общественных групп и активистов в различных частях света. Основная цель проекта – объединение с использованием возможностей ИКТ, в частности социальных сетей, организаций гражданского общества, распространяющих идеи о демократии, о правах человека, о защите окружающей среды и др., а также ведущих оппозиционную борьбу против авторитарных режимов.

Программа поиска **Enterprise Search** была введена в действие в 2004 г., обеспечивая доступ сотрудников Госдепа США к документам.

8.3.1.1.7. Программа «Idea Exchanges»

По инициативе госсекретаря США Х.Клинтон была создана **Комиссия по вопросам рационализации** в рамках программы **Idea Exchanges**, основная задача которой получение новых идей напрямую от сотрудников Госдепартамента США.

С момента запуска в феврале 2009 г. в комиссию было представлено свыше 2 500 идей. Страница программы служит форумом для обсуждения передовых практических методов.

[289] Civil Society 2.0. (http://www.state.goc/statecraft/cs20/).

Здесь размещаются такие уникальные сообщества, как, например, Инициатива экологизации дипломатии («Greening Diplomacy Initiative»), где пользователи имеют возможность делиться своими идеями о том, как улучшить экологическую обстановку в местах пребывания дипломатических миссий США.

На реализацию инновационных идей, поступивших от персонала, выделяется 2 млн. USD ежегодно из **Фонда инноваций**. В настоящее время эксперты Госдепа США уже одобрили ряд инновационных проектов: мобильное приложение для отслеживания качества воздуха в Гуанчжоу, сетевой экран с функциями антивируса для браузеров посольства в Минске, мобильный справочник по американским университетам для китайских студентов и др.

8.3.1.1.8. Социальные сети - новый алгоритм публичной дипломатии

Узел социальных сетей

Помимо эффективного управления накопленными знаниями **одной из основных задач Госдепа США является использование соцсетей, которые коренным образом изменили алгоритм публичной дипломатии.**

Правительство США эффективно управляет собственной глобальной медиа-империей: сообщения могут достигать аудитории в десятки миллионов человек, распространяясь через платформы более 600 соцсетей. Это дает возможность напрямую общаться с массовой аудиторией, не затрачивая при этом бюджетных средств на выстраивание каналов коммуникации. Государство также может извлечь пользу из сегментации аудитории, обмениваясь с тематическими группами сообщениями по поводу широкого спектра проблем: от противодействия терроризму до содействия продвижению экспертного научного знания в США.

Ключевым направлением одного из отделов Офиса электронной дипломатии - **узла социальных сетей (The Social Media Hub)** - является экспертная оценка социальных сетей и сетевых сообществ.

Задачи отдела состоят в следующем:

- поддержка сайта The Social Media Hub, где собраны методики и советы Госдепартамента по эффективной работе с социальными сетями, списки наиболее популярных социальных сетей в различных странах;

- консультирование дипломатических сотрудников работе с соцсетях, включая стратегию Госдепартамента в этой сфере;

- устранение проблем с аккаунтами, проведение интерактивных семинаров, разработка различных приложения и инструментов для публичной дипломатии.

В 2006 г. в Госдепартаменте появилась группа специалистов (**Digital Outreach Team**) для анализа сообщений и дискуссий, протекающих во всех возможных международных и национальных социальных сетях[290] в особенности в арабских социальных ресурсах, где настроения антиамериканизма развиты в наибольшей степени. Кроме этого, **специалисты Digital Outreach Team принимают участие в дискуссиях, регистрируясь в соцсетях в качестве рядовых участников или модераторов с целью разъяснения пользователям позиции США и ликвидации дезинформации, поступающей в сети со стороны противников США, таких как «Талибан» и «Аль-Каида». В зависимости от поставленных задач и целевой аудитории сотрудники отдела имеют возможность самостоятельно выбирать стиль и содержание публикуемых сообщений.**

Следует заметить, что в 2007-2008 гг. были созданы еще пятнадцать подобных отделов в Госдепартаменте США, ЦРУ, Министерстве обороны США, а также в Агентстве международного развития. Эти отделы занимаются анализом между-

[290] Digital Outreach Team (www.state.gov/iip/programs/)

народных и национальных социальных сетей, блогов, чатов, а также транслированием позитивной информации о США в сети Интернет[291].

Офис сетевой активности

Для освещения официальной позиции США в сети Интернет создан **Офис сетевой активности (Office of Web Engagement)**. Его основные задачи включают в себя управление несколькими платформами социальных сетей, включая 4 страницы Госдепартамента США в Facebook с аудиторией, превышающей миллион пользователей, электронный журнал о США (Ejournal USA), вызовы демократии (Democracy Challenge), глобальные дискуссии о климате (Global Conversations: Climate) и CO.NX.

Офис разрабатывает для этих страниц мобильные приложения, включая приложения, предназначенные для трансляции хода важных политических событий в социальных сетях. Сотрудники Офиса сетевой активности управляют различными сайтами на иностранных языках, включая арабский, китайский, фарси, французский, русский и испанский, созданные для улучшения имиджа США.

Проект **CO.NX** разработан для использования интерактивных веб-чатов и видео-чатов в различных дискуссиях Госдепартамента США: внутренних, межведомственных, а также публичных. Платформа CO.NX активно используется также для обучения сотрудников Госдепа США.

Центр электронных коммуникаций

Центр электронных коммуникаций осуществляет поддержку нескольких платформ социальных сетей **Госдепартамента США, предназначенных для ведения дискуссий**

[291] U.S. Public Diplomacy Actions Needed to Improve Strategic Use and Coordination of Research. GAO Report. 2007. P. 31.

на формальном уровне: блог DipNote, официальный Twitter-канал @StateDept, а также официальная страница Госдепа в Facebook. Сотрудники данного подразделения поддерживают официальные Twitter-каналы на арабском, китайском, фарси, французском, хинди, португальском, русском, испанском, турецком и урду.

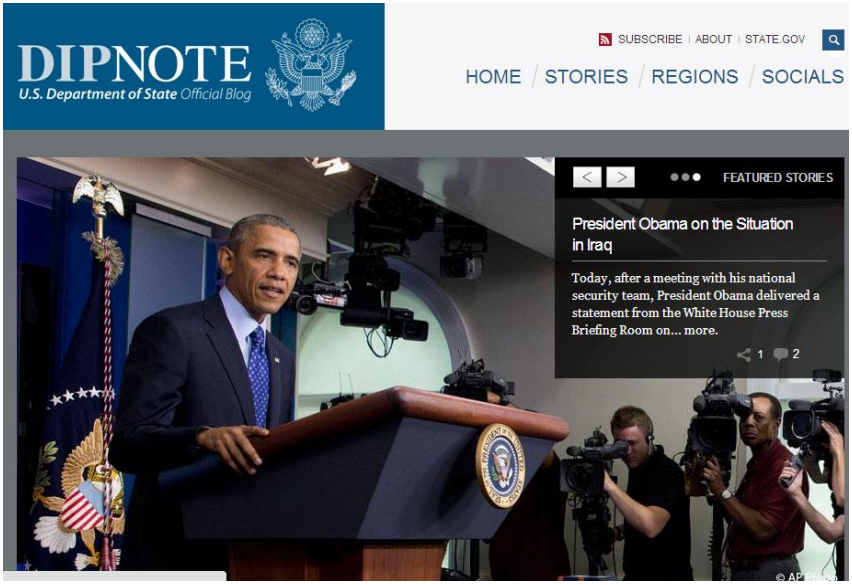


Рис. 8.4. Страница официального блога Госдепартамента США DIPNOTE[292]

Учитывая официальный характер данных сайтов, материал обычно проходит процедуру предварительного согласования, если необходимо информировать публику о позиции Госсекретаря по той или иной проблеме, или же подаются точные цитаты из материалов брифингов.

[292] https://blogs.state.gov/ 19.06.2014

Бюро по делам культуры и образования

Бюро по делам культуры и образования отвечает за масштабную программу культурных обменов в США в Отделе по публичным делам и стратегической коммуникации. Сотрудники Бюро поддерживают сайт Госдепартамента США **ExchangesConnect**, предназначенный для налаживания связей между потенциальными участниками программ обмена (американскими или иностранными гражданами) и выпускниками данных программ. В 2011 г. сайт насчитывал 37 000 участников.

Инструменты электронной дипломатии используются также в других подразделениях Госдепартамента США. Так, в рамках Офиса по инновационной деятельности создан **Отдел по исследованию аудитории** для разработки аналитических обзоров социальных сетей и обучению персонала Госдепа США работе в них.

Отдел быстрого реагирования

Для оценки реакции различных социальных сетей на процессы, потенциально имеющие значение для национальных интересов США, создан **Отдел быстрого реагирования**, сотрудники которого ежедневно формируют краткие аналитические отчеты на сей счет. Сотрудниками данного отдела ведется работа по фильтрации и проверке данных с Twitter, sms, электронной почты и RSS-каналов в режиме реального времени.

Вопросы консульского характера в рамках электронной дипломатии решаются с помощью веб-сайта travel.state.gov, а также его аккаунтов в Facebook и Twitter. Разработаны также приложения для мобильных телефонов на базе iPhone и Android.

8.3.1.1.9. Другие проекты Госдепартамента США

Программа **Эффект виртуального присутствия** (Virtual Presence Posts) позволяет смоделировать эффект виртуального дипломатического присутствия в городах, регионах и странах, где нет американских дипломатических миссий, с использованием сети Интернет.

В тесном сотрудничестве с другими подразделениями Госдепа США Офис электронной дипломатии осуществляет консалтинговые услуги в рамках программы **Collaboration Clearinghouse** по использованию передового мирового опыта в сфере ИКТ для содействия осуществлению внешнеполитических целей.

Среди планов и перспектив деятельности Офиса электронной дипломатии можно выделить следующие направления:

- объединить имеющиеся инструменты с тем, чтобы сотрудники Госдепа США имели возможность беспрепятственно получать информацию.
- разработать «умный» поиск информации с сохранением предыдущих запросов и возможностью обучения,
- объединить отчеты и другую информацию из таких проектов, как Communities@State, Diplopedia,
- улучшить поиск в Corridor, добавить опции уведомления и приглашения новых пользователей,
- обеспечить доступ к инструментам управления знаниями не только с рабочего места, но и в удаленном формате,
- запустить программу обучения персонала, в сотрудничестве с Институтом дипломатической службы.

8.3.1.1.10. The Foreign Affairs Network - глобальная сеть для всех загранучреждений США

The Foreign Affairs Network (FAN) – инновационный проект Госдепа США для обеспечения ИТ-услугами всех фе-

деральных агентств, размещенных за рубежом, с использованием общей сетевой платформы.[293]

Рис. 8.5. Foreign Affairs Network

Сеть FAN позиционируется как ответ на потребность в более безопасной, скоординированной и экономичной зарубежной ИТ-инфраструктуре.

Госдеп США предоставляет сетевые услуги таким пользователям, как Зарубежная сельскохозяйственная служба (Foreign Agricultural Service), Агентству пищевых продуктов и медикаментов (Food and Drug Administration), а также Агентству США по международному развитию USAID в 70 представительствах по всему миру.

Среди стандартных услуг, предоставляемых FAN, можно выделить следующие:

- доступ в Интернет
- печать
- сканирование

[293] http://www.state.gov/m/irm/c56714.htm 21.06.2014

- электронная почта
- сетевое файловое хранилище
- резервное копирование
- доступ к государственным сообщениям и архивной поисковой системе SMART
- обеспечение информационной безопасности

К дополнительным услугам относятся:

- служба удаленного доступа
- закупка оборудования
- видеоконференцсвязь
- логистические услуги и др.

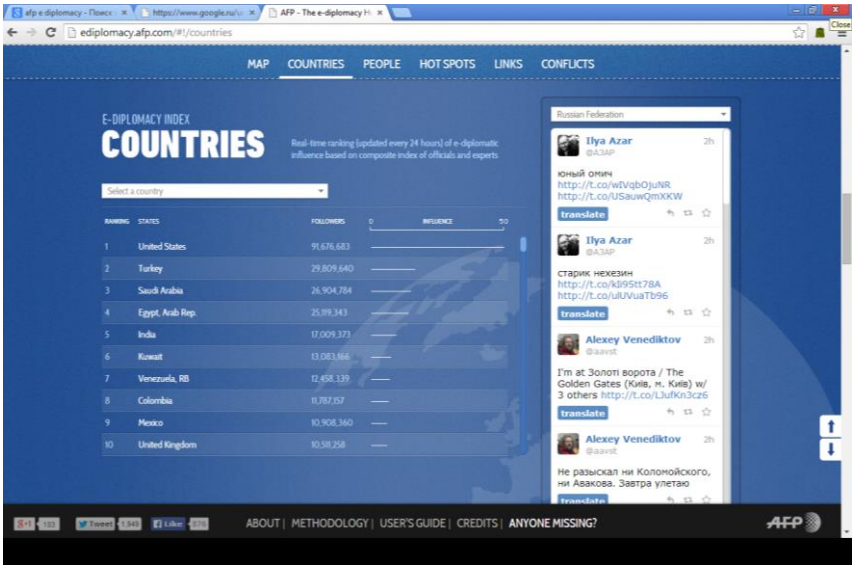
Глобальная сеть FAN поддерживает новейшие технологические изменения, что позволяет настраивать ее под конкретные задачи каждого участника. Госдеп США планирует расширять спектр предоставляемых данной сетью услуг для использования FAN в качестве сервиса для всех учреждений США, работающих за рубежом.

Таким образом, проведенный **анализ показывает, что Госдепартамент США опережает своих иностранных коллег по использованию мощного потенциала ИКТ**. Внедрение инструментов электронной дипломатии во внешней политике США является весьма результативным.

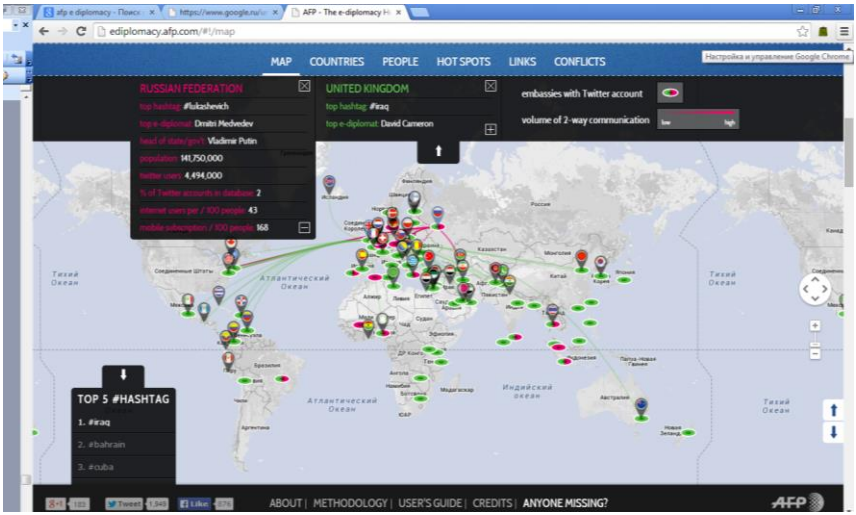
Развитие превентивных информационных стратегий, таких как мгновенная реакция правительства на негативную информацию о США в блогах, диалог между членами правительства США и отдельными блогерами, подавление экстремистской и террористической пропаганды, создание комплекса НПО посредством соцсетей, является одним из ключевых инструментов «мягкой силы 2.0» в реализации внешней политики США.

8.3.1.2. Великобритания

Согласно рейтингу АФП «E-Diplomacy», Великобритания входит в топ-10 стран с наибольшим количеством подписчиков на официальные аккаунты государства в Twitter (в Великобритании их более 10 511 000).[294]



[294] http://ediplomacy.afp.com/#!/map 21.06.2014



В целях повышения эффективности использования инновационных технологий во внешнеполитическом процессе в декабре 2010 г. в Великобритании была разработана Стратегия использования ИКТ на 2011-2015 гг. (ICT STRATEGY: 2011 – 2015)[295] для поддержки внешнеполитических приоритетов и дипломатического превосходства путем предоставления простых в использовании, гибких и высокоскоростных ИКТ-услуг.

Основными направлениями в реализации данной программы являются:

- модернизация имеющейся в МИД Великобритании безопасной и надежной ИТ-платформы с учетом требований информационной безопасности. Оказание ИТ-поддержки при использовании данной платформы организациям, осуществляющим свою деятельность за рубежом, в рамках политики правительства по консолидации корпоративных услуг;

[295] https://www.gov.uk/government/publications/fco-ict-strategy-2011-2015 20.06.2014

- руководствуясь внешнеполитическими приоритетами увеличение онлайн присутствия в Бразилии, Индии, Китае и других частях Азии, а также Турции и Индонезии;

- развертывание новой глобальной сети передачи данных и видеоконференцсвязи Echo[296], а также модернизация основной ИТ-платформы МИД Великобритании Firecrest.

- обучение сотрудников эффективному управлению знаниями и имеющейся информацией с использованием специального программного обеспечения.

В рамках настоящего исследования целесообразно рассмотреть также принятую в декабре 2012 г. «Цифровую» стратегию» МИД Великобритании (FCO Digital Strategy)[297], отражающую инновационные процессы, включая программы по созданию новейших информационных систем, в т.ч. по управлению знаниями, оснащению новейшим оборудованием, а также консульскую стратегию на 2013-2016 гг.

Так, согласно «Цифровой стратегии», МИД Великобритании имеет более 250 веб-сайтов загранпредставительств, в том числе 93 на иностранных языках, более 120 Twitter-каналов; более чем 120 страниц в Facebook, Flickr-канал, а также аккаунты в Flickr, Google+, YouTube, Instagram, Storify, Foursquare, Pinterest, LinkedIn, FCO podcasts, MixCloud, AudioBoo[298] и многочисленные местные или региональные цифровые каналы (например, Sina Weibo в Китае). В настоящее время семь руководителей МИД Великобритании и более 20 послов имеют аккаунты в Twitter. Сайт http://fco.gov.uk получил более 10 млн. просмотров страниц в 2012-13 гг.; более 100 тыс. подписчиков насчитывает Twitter–аккаунт министра иностранных дел.

[296] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/203169/gmpp-data-FCO-q2-2012-13.csv/preview

[297] FCO Digital Strategy https://www.gov.uk/government/publications/the-fco-digital-strategy

[298] https://www.gov.uk/government/organisations/foreign-commonwealth-office/about/social-media-use#uk-missions-to-international-organisations

В ноябре 2009 г. в МИД Великобритании было создано подразделение цифровой дипломатии, основной задачей которого является всестороннее использование ИКТ в дипломатии, при этом особое внимание уделяется работе с социальными сетями. Информация о деятельности данного подразделения доступна на портале «Цифровой дипломатии» МИД Великобритании по адресу:

http://blogs.fco.gov.uk/digitaldiplomacy/.

Посредством портала осуществляется оказание экспертной помощи и консультирование дипломатических сотрудников по вопросам цифровой дипломатии. Ресурс содержит также руководство по использованию инструментов цифровой дипломатии: инструкции по использованию Twitter, Facebook и других социальных сетей, по работе с веб-сайтом, размещению и подбору информационных, видео- и аудиоматериалов в сети, предусмотрен также раздел «Case-studies» с конкретными примерами реализованных проектов цифровой дипломатии.

Подразделение цифровой дипломатии МИД Великобритании насчитывает 15 сотрудников в центральном офисе, осуществляющих контроль за цифровым контентом, веб-платформой и цифровыми операциями; и 12 сотрудников за рубежом (в Индии, Сингапуре, Вашингтоне и Мадриде), занимающихся обновлением сообщений цифровых каналов, мониторингом качества услуг связи и др.[299]

МИД Великобритании предоставляет широкий спектр услуг в электронном виде: в т.ч. консультация британских граждан, выезжающих за рубеж (около 95% информации представлено на сайте); консульские услуги (около 25% от общего количества оказываемых услуг, 95% ответов на запросы консульского характера осуществляется в электронном виде, в т.ч. с использованием Twitter-канала @fcotravel; регистрация иностранных студентов, обучающихся в Великобри-

[299] FCO Digital Strategy https://www.gov.uk/government/publications/the-fco-digital-strategy. P. 7

тании; онлайн-оповещения туристов посредством SMS-сообщений.

Используя международный опыт, в МИД Великобритании создан кризисный центр, осуществляющий в т.ч. учет британских граждан, оказавшихся в кризисных ситуациях (100% реализация в электронном виде); информационную поддержку и помощь, оказываемую в Великобритании во время кризисных ситуаций (65% в эл.виде – в Великобритании, 10% - в стране пребывания), оповещения граждан осуществляются также через twitter-канал (@fcotravel. Кризисный центр в 2013 г. был номинирован на британскую премию «UK Agile Award»[300].

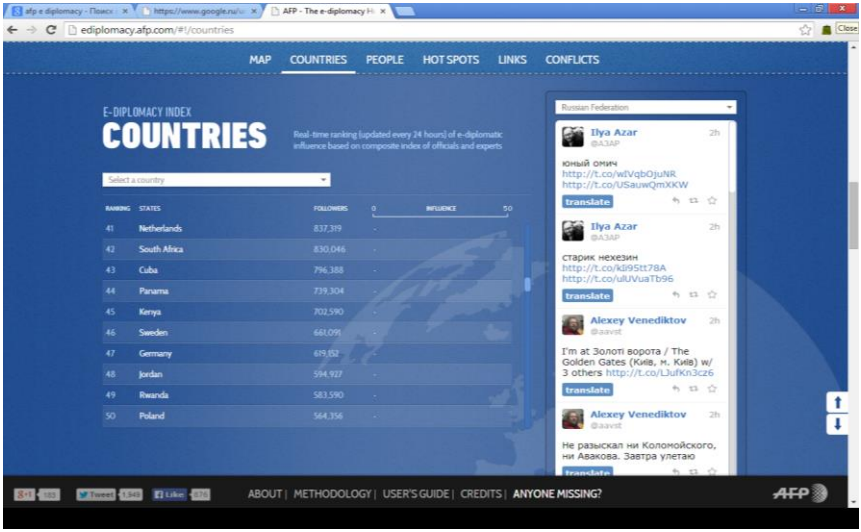
Отдельное направление деятельности - обучение сотрудников МИД Великобритании использованию цифровой дипломатии, а также обмену передовым ИКТ-опытом на местах. Это – разработка различных учебных программ для руководства и технического персонала, организация практических занятий с другими госорганами по использованию цифровых инструментов на практике; осуществление аудита использования ИКТ в повседневной работе.

Таким образом, реализация «Цифровой стратегии» МИД Великобритании позволит в полной мере выполнять новые задачи для обеспечения национальных интересов страны, повышения прозрачности и открытости внешнеполитической деятельности, наращиванию онлайн присутствия в мире путем, повсеместному использованию цифровых технологий в консульской работе и кризисном реагировании.

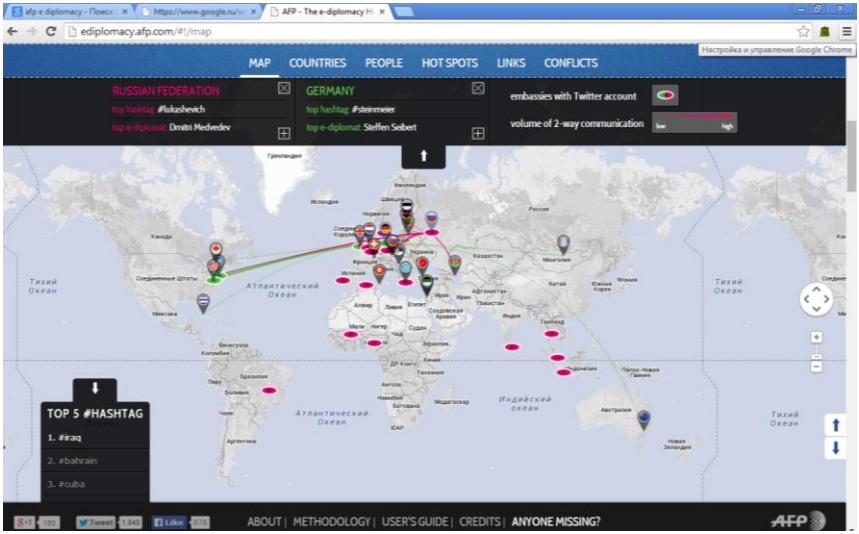
[300] http://blogs.fco.gov.uk/digitaldiplomacy/2013/12/20/foreign-office-digital-strategy-one-year-on/

8.3.1.3. «Цифровая» внешняя политика Германии

Согласно рейтингу AFP «E-Diplomacy» Германия находится на 47[301] месте и имеет более 627 тыс. подписчиков на Twitter-аккаунты.



[301] http://ediplomacy.afp.com/#!/map 21.06.2014



3 января 2014 г. на главной странице сайта МИД Германии[302] появилось сообщение о том, что министерство теперь в «цифровом мире» как «у себя дома».

Действительно, с мая 2011 г. МИД Германии имеет аккаунты в Twitter[303] (доступны по ссылкам @AuswaertigesAmt и @GermanyDiplo), с сентября 2012 г. - страницу в соцсети Facebook[304], а с октября 2012 г. – видеоканал в Youtube[305]. Более 70 немецких представительств за рубежом открыли «виртуальные посольства» в «Facebook», около 25 загранучреждений имеют аккаунты в «Twitter», используются и другие соцсети.[306]

При работе в социальных медиа немецкими загранпредставительствами учитываются региональные различия.

[302] http://www.auswaertiges-amt.de/DE/Startseite_node.html 21.06.2014
[303] http://www.auswaertiges-amt.de/DE/AAmt/00Aktuelles/110511-Twitter.html 19.06.2014
[304] http://www.auswaertiges-amt.de/DE/AAmt/00Aktuelles/121030_AA-auf-YouTube.html 19.06.2014
[305] http://www.auswaertiges-amt.de/DE/AAmt/00Aktuelles/121030_AA-auf-YouTube.html 19.06.2014
[306] http://www.auswaertiges-amt.de/DE/AAmt/ZuGastimAA/Aktuelles/140103-AA_Web2.0_Ueberblick.html 19.06.2014

Так, граждане Туниса активнее в соцсетях, в силу этого в миссиях были созданы аккаунты в Twitter и Facebook. В Китае активно используются микроблоги, поэтому представительства Германии представлены здесь на страницах «Weibo» (более 90 тысяч подписчиков) и "QQ". Представительства Германии в России присутствуют в соцсети «В контакте».

Для адекватного ответа на чрезвычайные и кризисные ситуации в МИД Германии функционирует Центр кризисного реагирования, осуществляющий свою деятельность в режиме 24/7 (подробно рассмотрен в п.7.2.3.1.).

В МИД Германии пристальное внимание уделяют вопросам обеспечения информационной безопасности. Отстаивание национальных интересов в сфере информационной безопасности в таких международных организациях, как ООН, ОБСЕ, Совет Европы, ОЭСР и НАТО, является одним из основных направлений стратегии информационной безопасности Германии.[307]

Ключевым моментом для «цифровой» внешней политики Германии является ее тесная связь с европейской «цифровой» политикой. При этом особое значение имеют следующие аспекты[308]:

- Интернет является двигателем и катализатором глобального экономического развития. Для этого создаются внешние условия таким образом, чтобы Германия могла воспользоваться «цифровыми» возможностями наилучшим образом.
- Необходимо сохранять в сети Интернет баланс между свободой и ответственностью. При этом должно соблюдаться верховенство закона без ограничения инновационного потенциала сети.

[307] http://www.auswaertiges-amt.de/DE/Aussenpolitik/GlobaleFragen/Cyber-Aussenpolitik/KS_Cyber-Aussenpolitik.html 21.06.2014
[308] http://www.auswaertiges-amt.de/DE/Aussenpolitik/GlobaleFragen/Cyber-Aussenpolitik/KS_Cyber-Aussenpolitik.html 21.06.2014

- Следует прилагать усилия для обеспечения максимальной безопасности в киберпространстве. Выявление и устранение угроз является целью комплексной оборонительной стратегии, за которую Германия выступает, в частности, в ЕС, ООН и ОБСЕ.

С учетом того, что «цифровая» внешняя политика затрагивает почти все направления деятельности министерства, в 2011 г. в МИД Германии был создан «Координационный штаб по «цифровой» внешней политике», осуществляющий свою деятельность в тесном сотрудничестве с другими заинтересованными госорганами.

Если я видел дальше других, то только потому,
что стоял на плечах гигантов

Исаак Ньютон

Вместо заключения. К цифровому миру без опасности: стратагемы для России

Проведенное исследование убедительно показало, что в условиях стремительного развития ИКТ, которое не мог предсказать даже самый смелый фантаст, проблема из технической трансформировались в сложнейшую геополитическую дилемму.

С одной стороны ИКТ - это несомненный потенциал и креативный двигатель цивилизации, с другой – столь быстро растущие вызовы и стратегические риски международной безопасности.

В этом контексте в докладе Группы правительственных экспертов ООН от 24 июня 2013 г. подчеркивается «Глобальный доступ, уязвимые технологии и фактор анонимности облегчают использование ИКТ в целях осуществления подрывной деятельности»[309]. В силу этого Россия выступила инициатором и стала локомотивом создания комплексной системы международной информационной безопасности в различных форматах сотрудничества: ООН, БРИКС, ОБСЕ, СНГ, ШОС, ОДКБ и других важных международных и региональных площадках.

Однако ИКТ стали и ключевым звеном шестого технологического уклада цивилизации - конвергенции нано-, био-, инфо- и когнотехнологий. Даже не эксперту понятно, что та страна, которая овладеет всем потенциалом НБИК-

[309] http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98 20.06.2014

технологий, способна получить неоспоримые преимущества в геополитической конкуренции.

Особую угрозу человечеству несет военно-политическая страта НБИК-технологий. Эта озабоченность нашла отражение в заявлении Секретаря Совета Безопасности России Н.П.Патрушева от 4 июля 2013 г. «О четвертой международной встрече высоких представителей, курирующих вопросы безопасности», состоявшейся 2 - 4 июля 2013 года в г.Владивостоке. По этой причине Россия призвала формировать новый эффективный международный механизм обеспечения безопасного развития и использования конвергентных технологий.[310]

В условиях глобального доступа попытка разделить международную и национальную информационную безопасность – это попытка провести черту по воде. Вот почему ведущие страны мира, наряду с международными, разрабатывают и реализуют национальные доктринальные и концептуальные стратагемы информационной или кибербезопасности.

По этой причине стратегически важна «Концепция общественной безопасности в Российской Федерации», утвержденная Президентом России 20 ноября 2013 г.[311]

В Концепции состояние общественной безопасности в России характеризуется как нестабильное.

В силу этого намечен широкий спектр мер, в т.ч. создание государственной системы мониторинга состояния общественной безопасности – единой межведомственной многоуровневой автоматизированной информационной системы, предназначенной для выявления, прогнозирования и оценки угроз общественной безопасности, оценки эффективности госполитики, а также для формирования предложений по совершенствованию состояния общественной безопасности.

[310] http://www.scrf.gov.ru/news/794.html 10.06.2014
[311] http://news.kremlin.ru/acts/19653 12.05.2014

Несомненно, что столь критически важная информационная система должна иметь мощный программно-технический комплекс информационной безопасности. С учетом межведомственного характера информсистемы возникает и институциональный вопрос – требуется введение должности ответственного за информационную безопасность (как в ряде стран: CISO - Chief Information Security Officer) на президентском или правительственном уровне.

Цифровая эпоха диктует свои правила обеспечения национальной безопасности в увязке с международной. Вот почему необходимо приложить максимум усилий по реализации «Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года».

Достижение согласия и учет взаимных интересов в процессе интернационализации глобального информационного пространства – категорический императив.

Альтернатива иррациональна – киберармагеддон!

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), Основы государственной политики в сфере МИБ (утв. Президентом РФ 24.07.2013), 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 общеевропейской 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 воз-

действия 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.

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 возможностей 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 Китая, 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 компью-

терному 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.*

Война́ - конфликт между политическими образованиями (государствами, племенами, политическими группировками и т. д.), происходящий в форме боевых действий между их вооружёнными 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 вооружённая 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 противо-

борствующей 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 телекоммуникационные 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; инфор-

мационных 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 к информации» возможность получения информации и ее использования.

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.

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

Информационная безопасность - состояние защищенности интересов личности, общества и государства от угроз деструктивных и иных негативных воздействий в информационном пространстве;

Информационная война - противоборство между двумя или более государствами в информационном пространстве с це-

лью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны;

Информационная инфраструктура - совокупность технических средств и систем формирования, преобразования, передачи, использования и хранения информации;

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

Информационное оружие - информационные технологии, средства и методы, предназначенные для ведения информационной войны;

Информационное пространство - сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию.

Информационно-коммуникационные технологии - совокупность методов, производственных процессов и программно-технических средств, интегрированных с целью формирования, преобразования, передачи, использования и хранения информации.

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.

Информационные ресурсы - информационная инфраструктура, а также собственно информация и ее потоки.

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.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Критически важный объект информационной инфраструктуры - часть (элемент) информационной инфраструктуры, воздействие на которую может иметь последствия, непосредственно затрагивающие национальную безопасность, включая безопасность личности, общества и государства;

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);

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.

Международная информационная безопасность - состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

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.

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) определённым нормам поведения и институтам на международной арене, что и приводит её 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 уровень 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;

Неправомерное использование информационных ресурсов - использование информационных ресурсов без соответствующих прав или с нарушением установленных правил,

законодательства государств либо норм международного права.

Несанкционированное вмешательство в информационные ресурсы - неправомерное воздействие на процессы формирования, обработки, преобразования, передачи, использования и хранения информации.

Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных

Правонарушение в информационном пространстве - использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях.

Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

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 кото-

рых 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.

Терроризм в информационном пространстве использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях;

Угроза в информационном пространстве (угроза информационной безопасности) - факторы, создающие опасность для личности, общества, государства и их интересов в информационном пространстве

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.

Организация Объединенных Наций A/RES/68/243

Генеральная Ассамблея

Distr.: General
9 January 2014

Шестьдесят восьмая сессия
Пункт 94 повестки дня

Резолюция, принятая Генеральной Ассамблеей 27 декабря 2013 года

[*по докладу Первого комитета (A/68/406)*]

68/243. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Генеральная Ассамблея,

ссылаясь на свои резолюции 53/70 от 4 декабря 1998 года, 54/49 от 1 декабря 1999 года, 55/28 от 20 ноября 2000 года, 56/19 от 29 ноября 2001 года, 57/53 от 22 ноября 2002 года, 58/32 от 8 декабря 2003 года, 59/61 от 3 декабря 2004 года, 60/45 от 8 декабря 2005 года, 61/54 от 6 декабря 2006 года, 62/17 от 5 декабря 2007 года, 63/37 от 2 декабря 2008 года, 64/25 от 2 декабря 2009 года, 65/41 от 8 декабря 2010 года, 66/24 от 2 декабря 2011 года и 67/27 от 3 декабря 2012 года,

ссылаясь также на свои резолюции по вопросу о роли науки и техники в контексте международной безопасности, в которых, в частности, признается, что достижения науки и техники могут иметь как гражданское, так и военное применение и что необходимо поддерживать и поощрять развитие науки и техники для использования в гражданских целях,

отмечая значительный прогресс, достигнутый в разработке и внедрении новейших информационных технологий и средств телекоммуникации,

подтверждая, что она видит в этом процессе широчайшие позитивные возможности для дальнейшего развития цивилизации, расширения возможностей взаимодействия на общее благо всех государств, увеличения созидательного потенциала человечества и дополнительных сдвигов к лучшему в распространении информации в глобальном сообществе,

напоминая в этой связи о подходах и принципах, которые были намечены на конференции «Информационное сообщество и развитие», состоявшейся в Мидранде, Южная Африка, 13–15 мая 1996 года,

13-45405

учитывая итоги Совещания на уровне министров по проблеме терроризма, которое состоялось в Париже 30 июля 1996 года, а также принятые на нем рекомендации[1],

учитывая также результаты Всемирной встречи на высшем уровне по вопросам информационного общества (первый этап — Женева, 10–12 декабря 2003 года, второй этап — Тунис, 16–18 ноября 2005 года)[2],

отмечая, что распространение и использование информационных технологий и средств затрагивают интересы всего международного сообщества и что широкое международное взаимодействие способствует обеспечению оптимальной эффективности,

выражая озабоченность тем, что эти технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на целостность инфраструктуры государств, нарушая их безопасность применительно как к гражданской, так и к военной сферам,

считая необходимым предотвратить использование информационных ресурсов или технологий в преступных или террористических целях,

отмечая важность уважения прав человека и основных свобод в сфере использования информационно-коммуникационных технологий,

отмечая вклад государств-членов, представивших Генеральному секретарю свои оценки по вопросам информационной безопасности в соответствии с пунктами 1–3 резолюций 53/70, 54/49, 55/28, 56/19, 57/53, 58/32, 59/61, 60/45, 61/54, 62/17, 63/37, 64/25 и 65/41, 66/24 и 67/27,

принимая к сведению доклады Генерального секретаря, содержащие эти оценки[3],

отмечая с удовлетворением инициативу Секретариата и Института Организации Объединенных Наций по исследованию проблем разоружения по проведению в Женеве в августе 1999 года и в апреле 2008 года международных встреч экспертов по вопросу о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также результаты этих встреч,

считая, что оценки государств-членов, содержащиеся в докладах Генерального секретаря, а также международные встречи экспертов способствовали лучшему пониманию существа проблем международной информационной безопасности и связанных с ними понятий,

учитывая, что во исполнение резолюции 66/24 Генеральный секретарь учредил в 2012 году на основе справедливого географического распределения группу правительственных экспертов, которая в соответствии со своим мандатом рассмотрела существующие и потенциальные угрозы в сфере информационной безопасности и возможные совместные меры по их устранению, включая нормы, правила или принципы ответственного поведения

---

[1] См. A/51/261, приложение

[2] См. A/C/2/59/3 и A/60/687.

[3] A/54/213, A/55/140 и Corr.1 и Add.1, A/56/164 и Add.1, A/57/166 и Add.1, A/58/373, A/59/116 и Add.1, A/60/95 и Add.1, A/61/161 и Add.1, A/62/98 и Add.1, A/64/129 и Add.1, A/65/154, A/66/152 и Add.1, A/67/167 и A/68/156 и Add.1.

государств и меры укрепления доверия в информационном пространстве, а также провела исследование соответствующих международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем,

с удовлетворением отмечая результативную работу Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и подготовленный в итоге соответствующий доклад, препровожденный Генеральным секретарем[4],

принимая к сведению оценки и рекомендации, содержащиеся в докладе Группы правительственных экспертов,

1. *призывает* государства-члены и далее содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также возможных стратегий по рассмотрению угроз, возникающих в этой сфере, исходя из необходимости сохранить свободный поток информации;

2. *полагает*, что целям таких стратегий соответствовало бы продолжение изучения соответствующих международных концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем;

3. *просит* все государства-члены продолжать, принимая во внимание оценки и рекомендации, содержащиеся в докладе Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности[4], информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:

a) общая оценка проблем информационной безопасности;

b) усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области;

c) содержание концепций, упомянутых в пункте 2 выше;

d) возможные меры, которые могли бы быть приняты международным сообществом для укрепления информационной безопасности на глобальном уровне;

4. *просит* Генерального секретаря с помощью группы правительственных экспертов, которая должна быть создана в 2014 году на основе справедливого географического распределения, продолжить с учетом оценок и рекомендаций, содержащихся в упомянутом выше докладе, в целях содействия выработке общего понимания исследование существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, включая нормы, правила или принципы ответственного поведения государств и меры укрепления доверия, вопросов использования информационно-коммуникационных технологий в конфликтах и того, как международное право применяется к использованию информационно-коммуникационных технологий государствами, а также концепций, упомянутых

[4] A/68/98.

в пункте 2 выше, и представить доклад о результатах данного исследования Генеральной Ассамблее на ее семидесятой сессии;

5. *постановляет* включить в предварительную повестку дня своей шестьдесят девятой сессии пункт, озаглавленный «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

72-е пленарное заседание,
27 декабря 2013 года

Приложение № 2
Оригинал: английский

975-е пленарное заседание
Журнал Постсовета № 975,
пункт 1 повестки дня

РЕШЕНИЕ № 1106

Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью снижения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий

Преамбульные параграфы

1. Государства-участники ОБСЕ в соответствии с Решением Постоянного Совета 1039 (26 апреля 2012 г.) договорились активизировать самостоятельные и коллективные усилия по обеспечению безопасности при всеобъемлющем и межизмеренческом использовании информационно-коммуникационных технологий (ИКТ) в соответствии с обязательствами в рамках ОБСЕ и во взаимодействии с соответствующими организациями, здесь и далее – безопасность при использовании ИКТ и самих ИКТ; было решено разработать проект комплекса мер укрепления доверия с целью повышения межгосударственного сотрудничества, транспарентности, предсказуемости и стабильности и уменьшения рисков ошибочного восприятия, эскалации и конфликтов, которые могут возникнуть в результате использования ИКТ;

2. Государства-участники ОБСЕ, признавая роль ОБСЕ в качестве региональной организации в соответствии с главой VIII Устава ООН, подтверждают, что разрабатываемые меры укрепления доверия дополняют общие усилия, предпринимаемые в рамках ООН в целях развития мер укрепления доверия в сфере безопасности при использовании ИКТ и самих ИКТ. Усилия государств-участников ОБСЕ при реализации мер укрепления доверия в сфере безопасно-

сти при использовании ИКТ и самих ИКТ в рамках ОБСЕ будут соответствовать международному праву, включая, среди прочего, Устав ООН и Международный пакт о гражданских и политических правах, а также Хельсинский заключительный акт, и их обязательствам по уважению прав человека и основных свобод.

Оперативные параграфы

1. Государства-участники на добровольной основе будут представлять свои национальные видения различных аспектов национальных и транснациональных угроз при использовании ИКТ и самим ИКТ. Объем такой информации будет определяться предоставляющими сторонами.

2. Государства-участники будут способствовать на добровольной основе развитию сотрудничества между компетентными национальными органами и обмену информацией в отношении безопасности при использовании ИКТ и самих ИКТ.

3. Государства-участники на добровольной основе и на соответствующем уровне будут проводить консультации с целью снижения риска ошибочного восприятия и возможного возникновения политических или военных напряженностей или конфликтов**,** которые могут возникнуть в результате использования ИКТ, и для защиты национальной и транснациональной критической инфраструктуры в сфере ИКТ.

4. Государства-участники на добровольной основе будут обмениваться информацией о предпринимаемых ими мерах по обеспечению открытого, обеспечивающего взаимодействие, безопасного и надежного Интернета.

5. Государства-участники будут использовать ОБСЕ как платформу для диалога и обмена наилучшими практиками, мерами повышения осведомленности и информацией о наращивании потенциала в отношении безопасности при использовании ИКТ или самих ИКТ, включая эффективное реагирование на соответствующие угрозы. Государства-

участники будут исследовать дальнейшее развитие роли ОБСЕ в связи с этим.

6. Государства-участники стремятся обеспечить наличие современного и эффективного национального законодательства в целях способствования на добровольной основе развитию двустороннего сотрудничества и эффективному и своевременному обмену информацией между компетентными органами, включая правоохранительные органы, в целях противодействия использованию ИКТ в преступных и террористических целях. Государства-участники ОБСЕ согласны с тем, что ОБСЕ не должна дублировать усилия, предпринимаемые по уже существующим между правоохранительными органами каналам.

7. Государства-участники на добровольной основе будут обмениваться информацией о своих национальных организациях, стратегиях или программах, включая сотрудничество между государственным и частным сектором, в отношении безопасности при использовании ИКТ и самих ИКТ в объеме, определяемом предоставляющей стороной.

8. Государства-участники назначат контактный пункт для установления связи и диалога по вопросам безопасности при использовании ИКТ и самих ИКТ. Государства-участники на добровольной основе будут предоставлять контактные данные официальных существующих национальных структур, в компетенцию которых входит реагирование на инциденты, связанные с применением ИКТ, и координировать ответы для установления прямого диалога и организация взаимодействия между уполномоченными национальными структурами и экспертами. Государства-участники будут обновлять контактную информацию ежегодно и сообщать об изменениях по прошествии не позднее 30 дней после внесения изменений. Государства-участники будут добровольно принимать меры по обеспечения оперативной связи на политическом уровне, чтобы разрешать озабоченности, возникающие на уровне национальной безопасности.

9. С целью снижения риска недопонимания в отсутствие согласованной терминологии и в целях продолжения диалога, Государства-участники на добровольной основе в качестве первого шага представят список национальных терминов, касающихся безопасности при использовании ИКТ и самих ИКТ вместе с объяснением или определением каждого термина. Каждое Государство-участник на добровольной основе само выберет те термины, которые оно сочтет наиболее подходящими для обмена. В качестве конечной цели Государства-участники будут прилагать все усилия для выработки консенсусного глоссария.

10. Государства-участники на добровольной основе будут осуществлять обмен взглядами с использованием площадок и механизмов ОБСЕ, среди прочего, Коммуникационную сеть ОБСЕ, обслуживаемую Центром предотвращения конфликтов Секретариата ОБСЕ, после принятия соответствующего решения ОБСЕ для установления связи по вопросам мер укрепления доверия.

11. Государства-участники на уровне государственных экспертов будут встречаться как минимум 3 раза в год в рамках Комитета по безопасности и его неформальной рабочей группы, созданной по решению № 1039 Постоянного Совета для обсуждения информации, обмен которой состоялся, и исследования возможностей надлежащего развития мер укрепления доверия. Вопросы для дальнейшего изучения неформальной рабочей группой могут включать, среди прочего, предложения из объединенного списка, разосланного под номером PC.DEL/682/12 9 июля 2012 г. председательством неформальной

Практические соображения

Положения настоящих Практических соображений не затрагивают принцип добровольности действий, связанных с вышеописанными мерами укрепления доверия.

Государства-участники ОБСЕ будут стремиться осуществить первый обмен информацией к 31 октября 2014 г., в дальнейшем обмен информацией, описанный в вышеупомянутых мерах укрепления доверия, будет происходить ежегодно. В целях достижения эффекта синергии дата проведения ежегодного обмена может синхронизироваться с соответствующими инициативами государств-участников в ООН и других площадках.

Каждое государство-участник объединяет информацию, которой предполагается обмениваться, перед ее представлением в один консолидированный блок. Информация предоставляется в наиболее транспарентном и удобном виде.

Государства-участники могут представлять информацию на любом из официальных языков ОБСЕ, сопровождая ее переводом на английский язык, либо только на английском языке.

Информация распространяется среди государств-участников через Систему распространения документов ОБСЕ.

В случае, если какое-либо государство-участник пожелает получить дополнительный комментарий по информации, представленной другим государством-участником, оно может сделать это в ходе заседаний Комитета по безопасности и его неформальной рабочей группы, созданной по решению № 1039 Постоянного Совета, или обратившись напрямую к государству, предоставившему эту информацию, через созданные контактные механизмы, включая список электронных адресов и дискуссионный форум POLIS.

Государства-участники будут реализовывать мероприятия, предусмотренные п.9 и п.10, через существующие органы и механизмы ОБСЕ.

Департамент по транснациональным угрозам будет, при поступлении обращения и в рамках существующих ресурсов, содействовать государствам-участникам в реализации вышеупомянутых мер укрепления доверия.

Реализуя меры укрепления доверия, государства-участники могут участвовать в дискуссиях и использовать знания и навыки, полученные в других профильных международных организациях, занимающихся вопросами, связанными с ИКТ.

Решение Постсовета/1106
3 декабря 2013 г.
приложение
Оригинал: русский

ИНТЕРПРЕТИРУЮЩЕЕ ЗАЯВЛЕНИЕ В СООТВЕТСТВИИ С ПУНКТОМ 6 РАЗДЕЛА IV. 1(A) ПРАВИЛ ПРОЦЕДУРЫ ОРГАНИЗАЦИИ ПО БЕЗОПАСНОСТИ И СОТРУДНИЧЕСТВУ В ЕВРОПЕ

Делегации Российской Федерации:

«В связи с принятым решением Постсовета о Первоначальном перечне мер укрепления доверия с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий и в соответствии с пунктом 6 раздела IV. 1(A) Правил процедуры ОБСЕ Российская Федерация хотела бы сделать следующее интерпретирующее заявление:

«Российская Делегация приняла активное участие в формировании консенсуса по данному важному решению. Его согласование, как известно, потребовало существенных усилий со стороны многих делегаций, участвовавших в переговорном процессе.

Поддержав это решение, Российская Федерация при его реализации будет исходить из твердой приверженности принципам невмешательства во внутренние дела государств, их равноправия в процессе управления Интернетом, суверенного права государств на управление Интернетом в национальном информационном пространстве, международному праву и соблюдению основных прав и свобод человека.

Прошу приложить текст настоящего заявления к принятому решению Постовета и включить его в Журнал сегодняшнего заседания».

Приложение № 3

Президент России

официальный сайт

Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия

17 июня 2013 года

Мы, президенты Российской Федерации и Соединенных Штатов Америки, признаем беспрецедентный прогресс в сфере использования информационно-коммуникационных технологий (ИКТ), новые возможности, которые они создают для экономик и обществ наших стран, и растущую взаимозависимость в современном мире.

Мы признаем, что угрозы в сфере использования ИКТ и самим ИКТ включают военно-политические и криминальные угрозы, а также угрозы террористического характера и относятся к ряду наиболее серьезных проблем национальной и международной безопасности, с которыми мы сталкиваемся в XXI веке. Мы подтверждаем важность сотрудничества между Российской Федерацией и Соединенными Штатами Америки, целью которого является укрепление взаимопонимания в этой области. Мы считаем, что это сотрудничество необходимо для обеспечения безопасности наших стран, а также для достижения в сфере использования ИКТ безопасности и надежности, существенно важных в плане инноваций и оперативной совместимости в глобальных масштабах.

Демонстрируя нашу приверженность содействию обеспечению международного мира и безопасности, сегодня мы подтверждаем завершение знаковых этапов, призванных укрепить отношения, повысить транспарентность и доверие между нашими двумя странами:

– в целях создания механизма обмена информацией для обеспечения более эффективной защиты критически важных информационных систем мы организовали канал связи и достигли договорен-

ностей по обмену информацией между нашими группами оперативного реагирования на компьютерные инциденты;

– для содействия обмену срочными сообщениями, которые могут снизить риск недопонимания, эскалации и конфликта, мы поручили использовать в этих целях линию прямой связи между нашими Центрами по уменьшению ядерной опасности;

– и, наконец, мы отдали распоряжение сотрудникам в Кремле и Белом доме установить между должностными лицами высокого уровня линию прямой связи по вопросам урегулирования потенциально опасных ситуаций, вызываемых событиями, которые могут создавать угрозы безопасности в сфере использования ИКТ и самим ИКТ.

Мы решили создать (в рамках российско-американской Президентской комиссии) двустороннюю рабочую группу по вопросам угроз в сфере использования ИКТ и самим ИКТ в контексте международной безопасности, которая будет встречаться на регулярной основе для проведения консультаций по вопросам, представляющим взаимный интерес и вызывающим взаимную озабоченность. Эта рабочая группа будет проводить оценку возникающих угроз, разрабатывать, предлагать и координировать конкретные совместные меры по реагированию на такие угрозы, а также по укреплению доверия. Эта группа должна быть сформирована в течение ближайшего месяца и безотлагательно приступить к практической деятельности.

Эти шаги необходимы для обеспечения наших национальных и более широких международных интересов. Они являются важными практическими мерами, которые могут содействовать дальнейшему продвижению норм мирного и законного поведения в отношении использования ИКТ на межгосударственном уровне. Для дальнейшего укрепления наших отношений соответствующие ведомства наших стран планируют продолжать регулярный диалог и определять дополнительные направления взаимовыгодного сотрудничества в области борьбы с угрозами в сфере использования ИКТ и самим ИКТ.

Приложение № 4

Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года

I. Общие положения

1. Настоящие Основы являются документом стратегического планирования Российской Федерации.

2. Настоящими Основами определяются основные угрозы в области международной информационной безопасности, цель, задачи и приоритетные направления государственной политики Российской Федерации в области международной информационной безопасности (далее - государственная политика Российской Федерации), а также механизмы их реализации.

3. Нормативную правовую базу настоящих Основ составляют Конституция Российской Федерации, международные договоры Российской Федерации в области международной информационной безопасности, федеральные законы, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, иные нормативные правовые акты Российской Федерации.

4. Настоящие Основы конкретизируют отдельные положения Стратегии национальной безопасности Российской Федерации до 2020 года, Доктрины информационной безопасности Российской Федерации, Концепции внешней политики Российской Федерации и других документов стратегического планирования Российской Федерации.

5. Настоящие Основы предназначены:

а) для продвижения на международной арене российских инициатив в области формирования системы международной информационной безопасности, включая совершенствование правового, организационного и иных видов ее обеспечения;

б) для формирования межгосударственных целевых программ в области международной информационной безопасности, в осуществлении которых участвует Российская Федерация, а также государственных и федеральных целевых программ в данной области;

в) для организации межведомственного взаимодействия при реализации государственной политики Российской Федерации в области международной информационной безопасности;

г) для достижения и поддержания технологического паритета с ведущими мировыми державами за счет более широкого использования информационных и коммуникационных технологий в реальном секторе экономики.

6. Под международной информационной безопасностью понимается такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

7. Под системой международной информационной безопасности понимается совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства.

Система международной информационной безопасности призвана оказать противодействие угрозам стратегической стабильности и способствовать равноправному стратегическому партнерству в глобальном информационном пространстве.

Сотрудничество в области формирования системы международной информационной безопасности отвечает национальным интересам Российской Федерации и способствует укреплению ее национальной безопасности.

8. Основной угрозой в области международной информационной безопасности является использование информационных и коммуникационных технологий:

а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

б) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

г) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

II. Цель и задачи государственной политики Российской Федерации

9. Цель государственной политики Российской Федерации заключается в содействии установлению международного правового режима, направленного на создание условий для формирования системы международной информационной безопасности.

10. Достижению цели государственной политики Российской Федерации будет способствовать участие Российской Федерации в решении следующих задач:

а) формирование системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях;

б) создание условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий для

осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

в) формирование механизмов международного сотрудничества в области противодействия угрозам использования информационных и коммуникационных технологий в террористических целях;

г) создание условий для противодействия угрозам использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств;

д) повышение эффективности международного сотрудничества в области противодействия преступности в сфере использования информационных и коммуникационных технологий;

е) создание условий для обеспечения технологического суверенитета государств в области информационных и коммуникационных технологий и преодоления информационного неравенства между развитыми и развивающимися странами.

III. Основные направления государственной политики Российской Федерации

11. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по формированию системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях, являются:

а) создание условий для продвижения на международной арене российской инициативы в необходимости разработки и принятия государствами - членами Организации Объединенных Наций Конвенции об обеспечении международной информационной безопасности;

б) содействие закреплению российских инициатив в области формирования системы международной информационной безопасности в итоговых документах, изданных по результатам работы

Группы правительственных экспертов Организации Объединенных Наций по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также содействие выработке под эгидой Организации Объединенных Наций правил поведения в области обеспечения международной информационной безопасности, отвечающих национальным интересам Российской Федерации;

в) проведение на регулярной основе двусторонних и многосторонних экспертных консультаций, согласование позиций и планов действий с государствами - членами Шанхайской организации сотрудничества, государствами - участниками Содружества Независимых Государств, государствами - членами Организации Договора о коллективной безопасности, государствами - участниками БРИКС, странами - членами Азиатско-тихоокеанского экономического сотрудничества, странами - членами «Группы восьми», «Группы двадцати», другими государствами и международными структурами в области международной информационной безопасности;

г) продвижение на международной арене российской инициативы в интернационализации управления информационно-телекоммуникационной сетью «Интернет» и увеличение в этом контексте роли Международного союза электросвязи;

д) организационно-штатное укрепление структурных подразделений федеральных органов исполнительной власти, участвующих в реализации государственной политики Российской Федерации, а также совершенствование координации деятельности федеральных органов исполнительной власти в данной области;

е) создание механизма участия российского экспертного сообщества в совершенствовании аналитического и научно-методического обеспечения продвижения российских инициатив в области формирования системы международной информационной безопасности;

ж) создание условий для заключения между Российской Федерацией и иностранными государствами международных договоров о сотрудничестве в области обеспечения международной информационной безопасности;

з) усиление взаимодействия в рамках Соглашения между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности и содействие расширению состава участников указанного Соглашения;

и) использование научного, исследовательского и экспертного потенциала Организации Объединенных Наций, других международных организаций для продвижения российских инициатив в области формирования системы международной информационной безопасности.

12. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию условий, способствующих снижению риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности, являются:

а) развитие диалога с заинтересованными государствами о национальных подходах к противодействию вызовам и угрозам, возникающим в связи с масштабным использованием информационных и коммуникационных технологий в военно-политических целях;

б) участие в выработке на двустороннем и многостороннем уровнях мер по укреплению доверия в области противодействия угрозам использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии;

в) содействие развитию региональных систем и формированию глобальной системы международной информационной безопасности на основе общепризнанных принципов и норм международного права (уважение государственного суверенитета, невмешательство во внутренние дела других государств, неприменение силы и угрозы силой в международных отношениях, право на индивидуальную и коллективную самооборону, уважение прав и основных свобод человека);

г) содействие подготовке и принятию государствами - членами Организации Объединенных Наций международных правовых актов, регламентирующих применение принципов и норм международного гуманитарного права в сфере использования информационных и коммуникационных технологий;

д) создание условий для установления международного правового режима нераспространения информационного оружия.

13. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по формированию механизмов международного сотрудничества в области противодействия угрозам использования информационных и коммуникационных технологий в террористических целях, являются:

а) развитие сотрудничества с государствами - членами Шанхайской организации сотрудничества, государствами - участниками Содружества Независимых Государств, государствами - членами Организации Договора о коллективной безопасности, государствами - участниками БРИКС, способствующего предупреждению, выявлению, пресечению, раскрытию и расследованию актов деструктивного воздействия на элементы национальной критической информационной инфраструктуры, минимизации последствий реализации таких актов, а также противодействию использования информационно-телекоммуникационной сети «Интернет» и других информационно-телекоммуникационных сетей в целях пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

б) содействие подготовке и принятию государствами - членами Организации Объединенных Наций акта, определяющего порядок обмена информацией о передовых практиках в области обеспечения безопасности функционирования элементов критической информационной инфраструктуры.

14. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию условий для противодействия угрозам использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств, являются:

а) участие в разработке и реализации межгосударственной системы мер по противодействию указанным угрозам;

б) содействие созданию международного механизма постоянного контроля за недопущением использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств.

15. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по повышению эффективности международного сотрудничества в области противодействия преступности в сфере использования информационных и коммуникационных технологий, являются:

а) продвижение на международной арене российской инициативы в необходимости разработки и принятия под эгидой Организации Объединенных Наций Конвенции о сотрудничестве в сфере противодействия информационной преступности, а также активизация работы с государствами - членами Шанхайской организации сотрудничества, государствами - участниками Содружества Независимых Государств, государствами - членами Организации Договора о коллективной безопасности, государствами - участниками БРИКС по поддержке данной инициативы;

б) развитие сотрудничества в сфере противодействия информационной преступности с государствами - членами Шанхайской организации сотрудничества, государствами - участниками Содружества Независимых Государств, государствами - членами Организации Договора о коллективной безопасности, государствами - участниками БРИКС, странами -членами Азиатско-тихоокеанского экономического сотрудничества, странами - членами «Группы восьми», «Группы двадцати», другими государствами и международными структурами;

в) повышение эффективности информационного обмена между правоохранительными органами государств в ходе расследования преступлений в сфере использования информационных и коммуникационных технологий;

г) совершенствование механизма обмена информацией о методиках расследования и судебной практике рассмотрения дел о преступлениях в сфере использования информационных и коммуникационных технологий.

16. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию условий для обеспечения технологического суверенитета государств в области информационных и коммуникационных технологий и преодоления информационного неравенства между развитыми и развивающимися странами, являются:

а) содействие разработке и реализации международных программ, способствующих преодолению информационного неравенства между развитыми и развивающимися странами;

б) содействие развитию национальных информационных инфраструктур и участию государств мирового сообщества в процессах создания и использования глобальных информационных сетей и систем.

IV. Механизмы реализации государственной политики Российской Федерации

17. Государственная политика Российской Федерации реализуется федеральными органами исполнительной власти и надзорными органами в соответствии с предметами их ведения при выполнении соответствующих межгосударственных целевых программ, в осуществлении которых участвует Российская Федерация, государственных и федеральных целевых программ, в том числе в рамках государственно-частного партнерства.

18. Подготовка предложений Президенту Российской Федерации по реализации основных направлений государственной политики Российской Федерации осуществляется рабочими органами Совета Безопасности Российской Федерации во взаимодействии с заинтересованными самостоятельными подразделениями Администрации Президента Российской Федерации, федеральными органами исполнительной власти и организациями.

19. Общая координация деятельности федеральных органов исполнительной власти, связанной с реализацией государственной политики Российской Федерации, а также с продвижением согласованной позиции Российской Федерации по этому вопросу на международной арене, осуществляется Министерством иностранных дел Российской Федерации.

* * *

20. Интенсивное развитие информационных и коммуникационных технологий, их широкое применение во всех сферах деятельности человека создали условия для формирования глобальной информационной инфраструктуры, которая предоставила качественно новые возможности социализации людей, их общения и доступа к накопленным человечеством знаниям.

В современном обществе информационные и коммуникационные технологии являются основным фактором, определяющим уровень социально-экономического развития и состояние национальной безопасности.

Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года призваны способствовать активизации внешней политики Российской Федерации на пути достижения согласия и учета взаимных интересов в процессе интернационализации глобального информационного пространства.

Приложение № 5

Unofficial translation

Basic principles

for State Policy of the Russian Federation in the field of International Information Security to 2020

I. General provisions

1. The Basic principles are a strategic planning document of the Russian Federation.

2. The Basic principles identify major threats in the field of international information security, the goal, objectives and priorities of state policy of the Russia Federation in the field of international information security (hereinafter – Russia's state policy) and mechanisms for their implementation.

3. The legal framework of the Basic principles includes the Constitution of the Russian Federation, international treaties and agreements of the Russian Federation in the field of international information security, federal laws, legal acts of the President of the Russian Federation and the Government of the Russian Federation and other legal instruments of the Russian Federation.

4. The Basic principles particularize selected provisions of National Security Strategy of the Russian Federation to 2020, Information Security Doctrine of the Russian Federation and Concept of the Foreign Policy of the Russian Federation, as well as other strategic planning documents of the Russian Federation.

5. These Basic principles are designed:

a) to promote internationally Russian initiatives to establish the international information security system, including through better legal, organizational and other support;

b) to develop intergovernmental target programs in the field of international information security involving Russia, as well as relevant state and federal task programs;

c) to build interagency cooperation in implementing state policy of the Russian Federation in the field of international information security;

d) to achieve and maintain technological parity with major world powers through an increased use of information and communications technologies in the real economy.

6. International information security is defined as such condition for the global information space which prevents any possibility of violation of rights of the individual, society and State in the information sphere, and destructive and unlawful impact on the elements of national critical information infrastructure.

7. International information security system is defined as a set of national and international institutions, which should regulate activities of different actors of the global information space.

International information security system should counter threats to strategic stability and facilitate equitable strategic partnership in the global information space.

Cooperation in the establishing of an international information security system is in line with the national interests of the Russian Federation and contributes to its national security.

8. The main threat in the field of international information security is the use of information and communications technologies:

a) as an information weapon for military and political purposes that are inconsistent with international law, for hostile actions and acts of aggression aimed at discrediting the sovereignty and violation of the territorial integrity of states and threatening international peace, security and strategic stability;

b) for terrorist purposes, including destructive impact on the elements of critical information infrastructure, as well as advocacy of terrorism and recruitment for terrorist activities;

c) for interference into the internal affairs of sovereign states, violation of public order, incitement of interethnic, interracial and interconfes-

sional strife, advocacy of racist and xenophobic ideas or theories that ignite hatred and discrimination and incite violence;

d) for committing crime, including those connected with unauthorized access to computer information, creation, use and dissemination of malicious computer software.

II. The Goal and Objectives of State Policy of the Russian Federation

9. The goal of state policy of the Russian Federation is to promote the establishment of the international legal regime aimed at creating conditions for the establishment of the system of international information security.

10. Participation of the Russian Federation in achieving the following objectives will contribute to accomplishing the goal of state policy of the Russian Federation:

a) to establish the international information security system on bilateral, multilateral, regional and global levels;

b) to facilitate the reducing of the risk of the use of information and communications technologies for hostile actions and acts of aggression that are aimed at discrediting the sovereignty and violating the territorial integrity of states and threatening international peace, security and strategic stability;

c) to launch the mechanisms of international cooperation on addressing threats of the use of information and communications technologies for terrorist purposes;

d) to create conditions for countering threats of the use of information and communications technologies for extremist purposes, including for interfering into the internal affairs of sovereign states;

e) to increase the efficiency of international cooperation on combating crime in the use of information and communications technologies;

f) to create conditions for exercising technological sovereignty of states in the use of information and communications technologies and overcoming information inequality between developed and developing countries.

III. Priorities of State Policy of the Russian Federation

11. Priorities of state policy aimed at establishment of the international information security system on bilateral, multilateral, regional and global levels are as follows:

a) to create conditions for promoting internationally the Russian initiative to develop and adopt the Convention on International Information Security by the United Nations Member States;

b) to ensure the enshrining Russian initiatives on the establishment of the international information security system in outcome documents adopted following the results of the work of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and contributing to elaboration of the rules of conduct in the field of international information security under the auspices of the United Nations that correspond to the national interests of the Russian Federation;

c) to hold regular bilateral and multilateral consultations of experts, to coordinate positions and action plans with Member States of the Shanghai Cooperation Organization, Participating States of the Commonwealth of Independent States, Member States of the Collective Security Treaty Organization, Member States of Asia-Pacific Economic Cooperation, BRICS States, G8 and G20 Member States, with other states and structures in the field of international information security;

d) to advance in the international arena Russia's initiative to internationalize the management of information and telecommunications network Internet and to enhance in this context the role of the International Telecommunication Union;

e) to enhance organizational and staff structure in the divisions of federal executive bodies which participate in implementing state policy of the Russian Federation, and to improve the coordination of federal executive bodies' activity in this sphere;

f) to launch a mechanism to involve Russian expert community advancement of analytical and methodological support of Russia's initiatives in establishing an international information security system;

g) to create environment for conclusion of international treaties and agreements on cooperation in the field of international information security between the Russian Federation and foreign states;

h) to enhance interaction within the framework of the Agreement between the Governments of Member States of the Shanghai Organization of Cooperation on cooperation in the field of provision of the international information security, and contributing to the expansion of the mentioned Agreement;

i) to harness scientific, research, and expert potential of the United Nations and other international organizations to advance Russia's initiatives in establishing an international information security system.

12. The priorities of state policy of the Russian Federation aimed at creation of conditions for reducing risks of use of information and communications technologies to carry out hostile activities or acts of aggression that discredit sovereignty, violate territorial integrity, and threaten international peace, security and strategic stability are the follows:

a) to promote dialogue with interested states on national approaches to address challenges and threats emerging from the large-scale use of information and communications technologies for military and political purposes;

b) to participate on bilateral and multilateral levels in elaboration of confidence-building measures to counter threats in the use of information and communications technologies to carry out hostile activities or acts of aggression;

c) to contribute to the development of regional systems and establishment of a global information security system based around universally recognized principles and standards of international law (respect for state sovereignty, non-interference into internal affairs of other states, refraining from the threat or use of force in international relations, right of individual and collective self-defense, respect for human rights and fundamental freedoms);

d) to promote formulation and adoption by Member States of the United Nations of international regulations concerning the use of principles and standards of international humanitarian law in the use of information and communications technologies;

e) creating environment for international legal regime of non-proliferation of information weapons.

13. The priorities of the state policy of the Russian Federation aimed at establishing mechanisms of international cooperation to counter the threats of using information and communications technologies for terrorist purposes are as follows:

a) to enhance cooperation with the Member States of Shanghai Cooperation Organization, Participating States of the Commonwealth of Independent States, Member States of Collective Security Treaty Organization and BRICS States that contributes to the prevention, detection, suppression, disclosure and investigation of destructive acts targeting the elements of national critical information infrastructure, to minimize the consequences of such acts, as well as to counter the use of Internet and other information and communication networks for the advocacy of terrorism and recruitment of terrorists;

b) to encourage the United Nations Member States to prepare and adopt an instrument defining the procedure for exchange of information on best practices to provide secure operation of the elements of critical information infrastructure.

14. The priorities of the state policy of the Russian Federation aimed at creating conditions for countering the threats in the use of information and communications technologies for extremist purposes, including interference into internal affairs of sovereign States are as follows:

a) to participate in the elaboration and implementation of international measures to counter the above mentioned threats;

b) to contribute to the establishment of an international mechanism for continuous monitoring to prevent the use of information and communications technologies for extremist purposes, including interference into internal affairs of sovereign States.

15. The principles of the state policy of the Russian Federation aimed at achieving a more effective international cooperation in countering cybercrime are as follows:

a) to promote the Russia's initiative to elaborate and adopt a convention on cooperation in combating cybercrime under the auspices of the United Nations on the international stage, as well as advance its work with the Member States of Shanghai Cooperation Organization, Participating

States of the Commonwealth of Independent States, Member States of Collective Security Treaty Organization and BRICS States to gain support for this initiative;

b) to enhance cooperation with the Member States of Shanghai Cooperation Organization, Participating States of the Commonwealth of Independent States, Member States of Collective Security Treaty Organization, BRICS States, Member States of the Asia-Pacific Economic Cooperation, G8 and G20 States, other States and international institutions in combating information crime;

c) to enhance the exchange of information between the law enforcement agencies of States in the course of investigation of crimes in the use of information and communications technologies;

d) to enhance the mechanism for exchange of information on investigation techniques and judicial practice concerning the crimes in the use of information and communications technologies.

16. The priorities of the state policy of the Russian Federation aimed at creating conditions for ensuring the technological sovereignty of States in the field of information and communications technologies and bridging the information gap between the developed and the developing countries are the follows:

a) to promote development and implementation of international programs designed to bridge the information gap between developed and developing countries;

b) to promote expansion of national information infrastructures and participation of nations of the world community in the creation and use of global information networks and systems.

IV. Mechanisms to Implement the State Policy of the Russian Federation

17. The state policy of the Russian Federation is realized by federal executive bodies and oversight bodies within their responsibility while implementing the corresponding interstate target programs, being carried out together with the Russian Federation, and the corresponding state and federal target programs, including public-private partnerships.

18. Proposals on the implementation of key provisions of the state policy of the Russian Federation are prepared for the consideration of the President of the Russian Federation by the working bodies of the Security Council of the Russian Federation in cooperation with relevant divisions of the Administration of the President of the Russian Federation as well as federal executive bodies and organizations.

19. The Ministry of Foreign Affairs of the Russian Federation is in charge of the overall coordination of the activities of federal executive authorities to implement the state policy of the Russian Federation and to promote the concerted position of the Russian Federation on the issue in the international arena of the information and communications technologies.

* * *

20. Rapid development and their expanded use in all areas of human activities, facilitated global information infrastructure that opened up new possibilities for people to socialize, communicate and get access to human knowledge.

In the modern society, information and communications technologies are the key determinant of the level of the social and economic development and the state of the national security.

Basic principles of the state policy of the Russian Federation in the field of the international information security to 2020 are intended to promote the foreign policy of the Russian Federation with a view to reach concord and to mutual interests in the process of internationalization of the global information environment.

Приложение № 6

Указ Президента Российской Федерации от 15 января 2013 г. N 31с

«О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

(Выписка)

В целях обеспечения информационной безопасности Российской Федерации постановляю:

1. Возложить на Федеральную службу безопасности Российской Федерации полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации - информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом.

2. Определить основными задачами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации:

а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

б) обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

3. Установить, что Федеральная служба безопасности Российской Федерации:

а) организует и проводит работы по созданию государственной системы, названной в пункте 1 настоящего Указа, осуществляет контроль за исполнением этих работ, а также обеспечивает во взаимодействии с государственными органами функционирование ее элементов;

б) разрабатывает методику обнаружения компьютерных атак на информационные системы и информационно-телекоммуникационные сети государственных органов и по согласованию с их владельцами - на иные информационные системы и информационно-телекоммуникационные сети;

в) определяет порядок обмена информацией между федеральными органами исполнительной власти о компьютерных инцидентах, связанных с функционированием информационных ресурсов Российской Федерации;

г) организует и проводит в соответствии с законодательством Российской Федерации мероприятия по оценке степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

д) разрабатывает методические рекомендации по организации защиты критической информационной инфраструктуры Российской Федерации от компьютерных атак;

е) определяет порядок обмена информацией между федеральными органами исполнительной власти и уполномоченными органами иностранных государств (международными организациями) о компьютерных инцидентах, связанных с функционированием информационных ресурсов, и организует обмен такой информацией.

4. Настоящий Указ вступает в силу со дня его подписания.

Президент Российской Федерации
В. Путин

Приложение № 7

Расшифровка беседы Нуланд и Пайета (с сайта радиостанции «Эхо Москвы»)

Нуланд: Что ты думаешь?

Пайет: Думаю, мы в игре. Вопрос с Кличко (лидер оппозиционной партии «Удар» - от ред.) , очевидно, это сложное звено здесь, в особенности объявление его заместителем премьер-министра. Ты видела некоторые мои заметки, насчет проблем сейчас во взаимоотношениях. Так что мы пытаемся быстро узнать, какую он играет роль. Так что думаю, твой аргумент для него, который тебе придется обозначить. Думаю, что наш следующий звонок, это был как раз тот, который ты провела с Яценюком.

Нуланд: Хорошо. Не думаю, что Кличко должен быть в правительстве. Не думаю, что это необходимо и что это хорошая идея.

Пайет: Да. С точки зрения того, что он не будет в правительстве, пусть остается и вне игры и занимается своей политической работой. Я просто думаю, если речь идет о продвижении процесса вперед, мы хотим сохранить умеренных демократов вместе. Проблема будет с Тягнибоком (лидер националистической партии «Свобода» - от ред.) и его ребятами. Я уверен, это частично то, на что рассчитывает Янукович и этой ситуации.

Нуланд: Я думаю, что Яценюк (лидер оппозиционной партии «Батькивщина» - от ред.) - это подходящий человек. У него есть опыт в экономических вопросах, в вопросах управления. Что ему нужно, так это чтобы Кличко и Тягнибок остались снаружи. Ему нужно разговаривать с ними четыре раза в неделю. Я просто думаю, что если Кличко попадет внутрь, будет на этом уровне работать на Яценюка, то это просто не получится.

Пайет: Да, я думаю, это так. Хорошо. Ты хотела бы, как следующий шаг, организовать телефонный разговор с ним?

Нуланд: Насколько я поняла из этого звонка, о котором ты мне говоришь, что трое лидеров были на своей собственной встрече, и что Яценюк собирался предложить в этом контексте разговор «три плюс один» или «три плюс два» с тобой. Ты же так это понял, не так ли?

Пайет: Нет. То есть он это предложил, однако думаю, что нет никакой динамики. Кличко был главным игроком, он будет еще долго ходить на все встречи, которые у них будут. Наверное, сейчас он как раз общается со своими ребятами. Думаю, если ты с ним напрямую свяжешься, это поможет разобраться с ролями всех троих. Также это дает тебе шанс быстро действовать в этой ситуации и обогнать нас. До того, как они …., и он объяснит, почему ему это не нравится.

Нуланд: Хорошо. Я согласна. Почему бы тебе не пообщаться с ним еще раз и не узнать, когда он хочет поговорить - до или после.

Пайет: Хорошо, так и сделаю. Спасибо.

Нуланд: Хорошо. Еще одно, Джеф. Не помню, говорила я тебе это, или говорила только Вашингтону. Когда я утром говорила с Джефом Фелтманом сегодня утром было новое имя для человека из ООН - Роберт Сери. Я писала тебе об этом утром.

Пайет: Да. Я видел.

Нуланд: Хорошо. Он теперь уговорил обоих - и Сери и Пан ги Муна, что Сери может приехать в понедельник или во вторник.

Пайет: Хорошо.

Нуланд: Думаю, это отлично поможет это все склеить. Замечательно, что ООН поможет это все склеить и проучить ЕС.

Пайет: Именно. Я думаю, нам нужно что-то сделать, чтобы склеить это все вместе. Потому что можно быть уверенным, что если это все начнет набирать обороты, россияне будут работать за кулисами, чтобы попытаться подорвать ситуацию.

И опять же. Тот факт, что это все там происходит, я все еще пытаюсь понять, почему Янукович сделал это. Однако в то же время сейчас идет встреча фракции Партии Регионов. Уверен, на данном этапе в этой группе идет оживленный спор.

В любом случае, мы можем сделать совместное решение, если будем действовать быстро. Давай я поработаю с Кличко. Думаю, нам нужно привлечь кого-то с международным именем, чтобы тот приехал и посодействовал с этим всем. Другой вопрос - как-то достучаться до Януковича. Но, наверное, мы подумаем об это завтра, когда увидим, как развиваются события.

Научное издание

ГЛОБАЛЬНАЯ БЕЗОПАСНОСТЬ
в ЦИФРОВУЮ ЭПОХУ:
СТРАТАГЕМЫ ДЛЯ РОССИИ

Под общей редакцией
Президента Национального института
исследований глобальной безопасности,
Председателя Отделения «Информационная глобализация»
Российской академии естественных наук,
доктора исторических наук, профессора
А.И. СМИРНОВА

Издано в авторской редакции

Подписано в печать 20.06.2014.
Формат 60x90/16. Усл. печ. л. 24,6.
Тираж 200 экз. Заказ № 30.

Отпечатано в ФГУП ГНЦ РФ «ВНИИгеосистем».
117105, Москва, Варшавское шоссе, 8.
Тел. 952-21-57. E-mail: artur@geosys.ru