В геологической истории биосферы
перед человеком открывается огромное будущее,
если он поймет это и не будет употреблять
свой труд и разум на самоистребление.

Академик В.И. ВЕРНАДСКИЙ

15-летию Российской академии
естественных наук посвящается

А. И. СМИРНОВ

ИНФОРМАЦИОННАЯ ГЛОБАЛИЗАЦИЯ и РОССИЯ: ВЫЗОВЫ и ВОЗМОЖНОСТИ

ПАРАД
ИЗДАТЕЛЬСКИЙ ДОМ
МОСКВА
2005

УДК 327
ББК 66.4
С 50

Рецензенты:
Доктор исторических наук Дегтярев А.Я.
Доктор технических наук, профессор Кретов В.С.
Зав.кафедрой Госуправления и информационных технологий Дипакадемии МИД России, канд. ист. наук Макаренко Г.Л.

А. И. Смирнов
С 50 Информационная глобализация и Россия: вызовы и возможности. — М.: Издательский дом «Парад», 2005. — 392 с.

ISBN 5-8061-0066-9

Книга освещает такие насущные проблемы геополитики, как становление информационной глобализации, роль мирового сообщества (ООН, ЮНЕСКО, Международный союз электросвязи, ОЭСР, «восьмерка», ЕС и др. региональные организации) в создании глобального информационного общества, национальный опыт ведущих стран по формированию электронного правительства, особенности пути к информационному обществу России, продвижение Россией решения проблемы международной информационной безопасности, в т.ч. в контексте борьбы с международным терроризмом.

Книга позиционирует новейшие теоретические и практические наработки на стыке информационно-коммуникационных технологий и международных отношений к новым вызовам и угрозам цивилизации и может быть полезна для широкого круга читателей, интересующихся столь актуальным направлением геополитики.

Anatoly I.Smirnov
Information globalization and Russia: challenges and opportunities.

The book contents such essential problems of geopolitics as becoming of information globalization, a role of the international community (UN, UNESCO, ITU, OECD, “G8”, EU, etc.) in creation of a global information society, national experience of the leading countries on formation of “e-government”, feature of a way to an information society of Russia, promotion of the decision of a problem of the international information safety by Russia, including in context of struggle against the international terrorism.

The book has the newest theoretical and practical operating time on a joint of information-communication technologies and the international attitudes to new challenges and threats of a civilization and can be useful for a wide range of the readers, were interested so actual direction of geopolitics.

ISBN 5-8061-0066-9

ВВЕДЕНИЕ

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

А. ЭЙНШТЕЙН

Вот уже более полувека весь мир охвачен беспрецедентной информационной революцией, которая все более отчетливо позиционируется как локомотив глобализации.

Феномен резко возрастающего влияния информационно-коммуникационных технологий (ИКТ) на формирование общества XXI века был отмечен в Окинавской Хартии глобального информационного общества, принятой лидерами «восьмерки» 22 июля 2000 г.[1] Наиболее полно он исследуется в проходящей под эгидой ООН и Международного союза электросвязи (МСЭ) Встрече в верхах по глобальному информационному обществу (ВВГИО), первый этап которой состоялся в Женеве в декабре 2003 г., а второй — в ноябре 2005 г. в Тунисе.

Проблематике информационного общества и глобализации посвящено огромное количество конференций, симпозиумов, а также исследований и публикаций на многих иностранных языках, в

[1] Окинавская Хартия глобального информационного общества // Дипломатический вестник. 2000. № 8. С. 52.

т.ч. в сети Интернет. Россия за последнее десятилетие приложила немалые усилия, чтобы сократить разрыв от таких признанных государств-лидеров в ИКТ, как Великобритания, Дания, Норвегия, Сингапур, США, Финляндия, Южная Корея, Япония и ряд других стран.

Политические аспекты данной проблематики рассматриваются, в частности, в работах отечественных авторов Абдеева Р.Ф., Барановского Е.Г., Вершинской О.Н., Галумова Э. А., Иноземцева В.Л., Ершовой Т.В., Засурского Я.Н., Кашлева Ю.Б., Лебедевой М.М., Мелюхина И.С., Модестова С.А., Панарина А.С., Чернова А.А. и др[2].

Вопросы правового обеспечения процесса становления глобального информационного общества затрагиваются в работах Ефимовой Л.Л., Кристального Б.В., Соловяненко Н.И., Якушева М.В. и др[3]. Экономическая компонента этого процесса рассматривается в трудах Делягина М.Г., Жданова В.С., Стрелец И.А., Фролова С.В., а также ряда других исследователей[4]. Проблемы обеспечения информационной безопасности поднимаются в работах таких авторов, как Зуев А.,

---

[2] *Абдеев Р.Ф.* Философия информационной цивилизации. М.: ВЛАДОС, 1994; *Барановский Е.Г., Владиславлева Н.Н.* Методы анализа международных конфликтов. М.: Научная книга, 2002; *Вершинская О.Н.* Существующие модели построения информационного общества // Информационное общество. 1999. № 3; *Ершова Т.В.* Российский опыт интеграции в информационное общество // Информационное общество. 1999. № 1; *Иноземцев В.Л.* Современное постиндустриальное общество: природа, противоречия, перспективы. М.: Логос, 2000; *Засурский Я.Н.* Информационное общество и СМИ // Информационное общество. 1999. № 1; *Кашлев Ю., Галумов Э.* Информация и PR в международных отношениях. М.: Известия, 2003. 432 с.; *Лебедева М.М.* Современные технологии и политическое развитие мира // Международная жизнь. 2001. № 2; *Мелюхин И.С.* Информационное общество: истоки, проблемы, тенденции развития. М.: Изд-во МГУ, 1999. 208 с.; *Модестов С.А.* Информационное противоборство как фактор геополитической конкуренции. М., 1994.; *Панарин А.С.* Глобализация как вызов жизненному миру // Вестник РАН. 2004. Т. 74. С. 619–632.; *Чернов А.А.* Становление глобального информационного общества: проблемы и перспективы. М.: «Дашков и К», 2003. 232 с.

[3] *Ефимова Л.Л.* Особенности правового обеспечения информационной безопасности на телевидении и радиовещании // Информационное общество. 2000. № 3; *Кристальный Б.В.* Концепция закона РФ «Об электронной торговле» // Информационное общество. 2000. № 3; 1999. № 6; *Якушев М.В.* Информационное общество и правовое регулирование: новые проблемы теории и практики // Информационное общество. 1999. № 1.

[4] *Делягин М.Г.* Мировой кризис: Общая теория глобализации. М.: ИНФРА, 2003. *Жданов В.С.* Электронная коммерция // Информационное общество. 1999. № 5; *Стрелец И.А.* Новая экономика и информационные технологии. М.: «Экзамен», 2003; *Фролов С.В.* Бизнес в Интернете // Информационное общество. 1999. № 2.

Крутских А.В., Панарин И.Н., Райков А.Н., Стрельцов А.А., Черешкин Д.С., Федоров А.В. и др[5].

Среди зарубежных авторов по излагаемой проблематике заслуживают особого внимания работы Д. Белла (D. Bell), К. Вербаха (K. Werbach), М.Кастельса (M.Castells), Э. Кинга (E. King), И. Масуды (Y. Masuda), Т. Меррилла (T. Merrill), М. Пората (M. Porat), Л. Робертса (L. Roberts), К. Робинсона (K. Robinson), Р. Рэддика (R. Reddick), А.Тоффлера (A. Toffler) и др.[6]

Особого внимания в данном списке заслуживает рассекреченный в начале 2005 года документ под названием «Контуры мирового будущего: Доклад по проекту — 2020 Национального разведывательного совета США»[7]. Это третий за последние годы рассекреченный доклад американского Национального разведывательного совета, в котором предпринимается попытка достаточно долгосрочного обзора будущего. Масштабность изменений, которые могут произойти за 15 лет, можно представить, оглянувшись на 15 лет назад: в 1990 году на геополитической карте еще существовало государство СССР, про Интернет слышали лишь единицы.

---

[5] *Зуев А.* Безопасность в виртуальном пространстве // Мировая экономика и международные отношения. 2003. № 9; *Крутских А., Федоров А.* О международной информационной безопасности // Международная жизнь. 2000. № 2; *Панарин И.Н.* Информационные войны и Россия // Информация. Дипломатия. Психология: Сборник материалов «круглого стола» и лекций преподавательской кафедры массовой коммуникации и связей с общественностью Дипломатической академии МИД России. М., 2002; *Райков А.Н.* Информационная безопасность и управление // Информационное общество. 1999. № 5; *Сергиенко Л.А.* Защита персональных данных в Интернет // Информационное общество. 2000. № 5; *Стрельцов А.А.*Обеспечение информационной безопасности России. Теоретические и методологические основы. М.: МЦНМО, 2002. 296 с. *Черешкин Д.С.* Проблемы управления информационной безопасностью. М.: Едиториал УРСС, 2002. 224 с.

[6] *Bell D.* The Coming of Post-industrial Society. A Venture in Social Forecasting. N.Y.: Basic Books, Inc., 1973; *Кастельс М.* Информационная эпоха: экономика, общество и культура. М.: ГУ ВШЭ, 2000. 608 с. *Masuda Y.* The Information Society as Postindustrial Society. Washington.: World Future Soc., 1983; *Porat M., Rubin M.* The Information Society: Development and Measurement. Washington, 1978; *Reddick R., King E.* The Online Journ@list: Using the Internet and Other Electronic Resources. FACS. London, 1996; *Robinson K.G.* Building a Global Information Society // Aspen Institute, 1996; *Werbach K.* Digital Tornado: The Internet and Telecommunications Policy. USA. Federal Communication Commission, 1997; *Roberts L., Merrill T.* Toward a Cooperative Network of Time-Shared Computers. Fall AFIPS Conf. Oct., 1996; *Tofler A., Toffler H.* Creating of New Civilization: the Politics Of 0the Third Wave. Atlanta, 1995. 112 p.

[7] См. Россия и мир в 2020 году: Доклад Национального разведывательного совета США «Контуры мирового будущего»; *А. Шубин* Россия-2020: будущее страны в условиях глобальных перемен. М.: «Европа», 2005.

Американский доклад, подготовленный по заказу ЦРУ, ничего не предсказывает, однако намечает основные пути и проблемы развития нашей цивилизации и предлагает несколько возможных вариантов будущего. Узловые факторы в переменах, обусловленных глобализацией, разработчики доклада видят следующие: противоречия самой глобализации; подъем новых держав (в частности, Китая и Индии) и перемены в связи с этим в геополитическом пейзаже; новые проблемы управления (в частности, государства-нации будут подвергаться все возрастающему давлению со стороны более глобальных, в том числе виртуальных, сообществ, корпораций, наднациональных религиозных объединений) и, наконец, — «всеобъемлющее чувство ненадежности», которое, по мнению американского разведывательного сообщества, все больше влияет на формирование мира.

За этими общими характеристиками можно увидеть «ряд специфических взаимоисключающих тенденций: расширение мировой экономики, ускоренные темпы научного прогресса и распространение технологий двойного назначения, сохранение социального неравенства, появление новых держав, феномен глобального старения, замедление процесса демократизации, распространение радикальной исламской идеологии, потенциальная возможность катастрофического терроризма, распространение оружия массового поражения, усиление давления на международные институты». Во второй части книги — статья А. Шубина «Россия-2020: будущее страны в условиях глобальных перемен», где исследуются сценарии будущего для нашей страны.

Анализ резко ускоряющихся всеохватывающих коммуникативных процессов глобализации показывает, что они эволюционируют в качественно новое состояние – режим реального времени. В силу этого в книге они рассматриваются под уже известным понятием ***информационная глобализация***.

В предлагаемой монографии исследуются некоторые теоретические и практические компоненты информационной глобализации, ее тенденции и доминанты, а также порождаемые ею вызовы и возможности для национальных интересов России. На базе современной информации в работе предпринята попытка проанализировать международный опыт создания информационного общества и электронного правительства, а также их различных моделей.

Отдельная глава посвящена особенностям формирования информационного общества в России, в т. ч. в контексте осуществляемой административной реформы. В заключительной главе ис-

следуется внешнеполитический аспект подходов России к проблеме глобального информационного общества, включая инициативы России в ООН по продвижению концепции международной информационной безопасности в качестве ответа на новые вызовы и угрозы, в т.ч. со стороны международного терроризма.

На основе проведенного исследования в заключении формулируются выводы о проблемах и перспективах интеграции России в глобальное информационное общество.

С учетом того, что понятийный аппарат по данной проблематике еще недостаточно отработан, в книге приводится глоссарий по наиболее часто встречающимся терминам и дефинициям. Представляется, что востребованным для читателя станет и приложение, содержащее основополагающие документы по излагаемой проблеме, как российских структур и организаций, так и международных.

Автор выражает искреннюю признательность Дипломатической академии МИД России, в том числе кафедре Государственного управления и информационных технологий за оказанную помощь, а также уважаемым рецензентам за ценные замечания и рекомендации, высказанные относительно монографии.

Глава 1
ГЛОБАЛИЗАЦИЯ И ИНФОРМАЦИОННОЕ ОБЩЕСТВО

Информационное общество —
это такой этап истории человечества,
когда коллективный разум становится
не только опорой развития Homo sapiens,
но и объектом целенаправленных усилий
по его совершенствованию.

Академик Н.Н. МОИСЕЕВ

1.1. Информационно-коммуникационные технологии — локомотив и нерв глобализации

Цивилизация стремительно вступила в новую эру своего развития. Постулируемый тезис подтверждается нижеследующим синопсисом ее эволюции. По некоторым оценкам человечество обитает на планете более 50 тысяч лет, в течение которых сменилось порядка 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 время;
- 6 — используют искусственные источники энергии;
- 4 — пользуются электромоторами;
- 2 — владеют атомной энергией, реактивной авиацией, телевидением, лазерами, антибиотиками.

И только **одно поколение** применяет персональные компьютеры, космические технологии, телекоммуникацию, Интернет, генную инженерию![1] Это же поколение вступило в активную стадию многомерного процесса **глобализации**.

В этом контексте еще более ошеломляюще звучит прогноз Б.Гейтса, данный в первой строке переведенной на русский язык его книги «Бизнес со скоростью мысли»: «В ближайшие 10 лет бизнес изменится сильнее, чем за предыдущие пятьдесят»[2]. Естественно, Б.Гейтс, располагая немалой конфиденциальной информацией о новейших разработках и перспективах компьютерных технологий, может с достаточно высокой долей уверенности утверждать о феномене революционного влияния ИКТ на бизнес и процессы глобализации мирового развития в целом.

1.1.1. Глобализация – pro et contra

К процессам глобализации в последнее время приковано внимание ведущих политиков, политологов и экономистов всего мира. **Оценки развития глобализации от восторженных постепенно смещаются к попыткам объяснения тех негативных явлений, которые становятся все более заметными в его «триумфальном шествии», поиску рецептов их преодоления и адекватных ответов на выпады антиглобалистов**[3].

Применительно к политике США эту метаморфозу можно проследить, в частности, на примере последнего труда З.Бжезинского «Выбор:

---

[1] См. http://www.nasled.ru/pressa/isdaniya/global_1/pril_7.html

[2] *Гейтс Б.* Бизнес со скоростью мысли. М.: ЭКСМО-Пресс, 2000. С.12

[3] См. *Дахин В.Н., Проскурин С.А.* Политические проблемы глобализации. РАГС. М., 2003.

господство или лидерство»[4]. Мэтр политологии, десятилетиями создававший доктрину глобального превосходства США, ставит вопрос: что последует, если «нынешнее американское глобальное превосходство... в определенный момент — который может наступить гораздо раньше, чем это допускается многими американцами, — исчезнет»? Суть же его предложения состоит в том, что США должны перейти от «одностороннего доминирования» к тому, что он называет «консенсусным лидерством». Автор призывает Америку к сознательной сдержанности на мировой арене, к тому, чтобы быть более внимательными к опасностям, вытекающим из отождествления американских интересов с несправедливостями глобализации, которое может породить всемирную реакцию, воплощающуюся в формировании идеологии антиамериканизма.

Существует немало самых разнообразных дефиниций глобализации. В контексте проблематики данной книги наиболее емкое определение дал известный экономист М.Г.Делягин в резюме к своему фундаментальному труду «Мировой кризис: Общая теория глобализации»: ***«Глобализация – процесс лавинообразного формирования единого общемирового финансово-информационного пространства на базе новых, преимущественно компьютерных, технологий»[5].*** Схожее определение дает другой исследователь информационной глобализации И.А.Стрелец[6].

Эксперты сходятся во мнении, что впервые понятие «глобализация» ввел профессор Гарвардской школы бизнеса Т. Левитт в статье «Глобализация рынков» в 1983 г.[7] Он считал, что глобализация и технологии стали главными факторами, определяющими международные отношения.

Крупный японский специалист в области стратегии управления К.Омаэ в книге «Власть Триады» (1985 г.) назвал «Триадой» треугольник, образованный США, Японией и Западной Европой. Он показывает, что для выживания в условиях жестокой конкуренции, сложившейся в странах Триады, многонациональные корпорации должны обладать глобальным видением и действовать в глобальном измерении[8].

---

[4] *Бжезинский З.* Выбор: господство или лидерство. М., 2004.

[5] *Делягин М.Г.* Мировой кризис: Общая теория глобализации: Курс лекций. М.: ИНФРА, 2003.

[6] *Стрелец И.А.* Новая экономика и информационные технологии. М.: «Экзамен», 2003. С. 42.

[7] *Theodore Levitt.* The Globalization of Markets // Harvard Business Review. May-Juin. 1983. P. 92–93.

[8] *Kenichi Ohmae.* Triad Power. The Coming Shape of Global Competition // Free Press. New York. 1985.

Позднее термин «глобализация» стал применяться для описания взрывообразного процесса передвижения капиталов и интеграции финансовых и биржевых рынков вследствие бурного развития ИКТ.

Окончание холодной войны, возрастание экономической взаимозависимости, возросшие экологические угрозы, которые породили понимание единой планеты, привели к расширению понятия «глобализация», придав ему политическую, социальную, историческую, географическую и культурную составляющую.

Заслуживает внимания то, что в некоторых странах, например во Франции, термином «глобализация» обозначают экономические и финансовые характеристики более глобального процесса — мондиализации. Французские эксперты, не только в силу лингвистического неприятия американизмов, полагают, что мондиализация является завершением интернационализации и отличается от глобализации, которая к стиранию расстояний и барьеров добавляет стирание понятия времени, ставшее возможным благодаря ИКТ.

Интересна позиция У. Бека, который в книге «Что такое глобализация?» считает, что глобализация была наиболее широко используемым, в том числе неверным образом, ключевым словом в дискуссиях в последние годы и станет им в предстоящие годы. При этом оно наиболее часто неправильно интерпретируется, являясь в то же время наиболее политически эффективным понятием. У.Бек призывает различать ряд измерений глобализации, при этом любой их перечень должен включать коммуникационные технологии, экологию, экономику, организацию деятельности, культуру и гражданское общество[9].

Некоторые исследователи считают, что процесс глобализации начался значительно раньше. Так, Ф.Дефарж пишет, что именно Великие географические открытия, совершенные европейцами, положили начало глобализации. Достижения XIX века — индустриальная революция, революция в транспорте и демографические изменения — расширили и ускорили процесс глобализации. Закрепили формирование мировой геополитической арены две мировые войны XX века и три глобальных потрясения: деколонизация, появление глобальной системы международного обмена в сфере торговли, финансов и технологий, а также включение посткоммунистических государств и стран «третьего мира» в международные экономические отношения. Неотъемлемой чертой глобализации,

[9] *Ulrich Beck*. What is Globalization? Cambridge. UK. 2000. P. 19-20.

утверждает автор, является взрывообразный характер передвижения всех видов потоков: капитала, людей, технологий, услуг, информации и идей[10].

Представляется важной позиция по периодизации глобализации Организации экономического сотрудничества и развития (ОЭСР), которой эксперты давали самые разные определения: научный центр, контролирующий орган, клуб 30 наиболее богатых стран, практический университет[11]. ОЭСР выделяет следующие три этапа в процессе глобализации:

- интернационализация (с середины XIX века — развитие экспортных потоков);
- транснационализация (с 1945 года – в связи с резким ростом объемов инвестиций и их размещением в зарубежных странах);
- глобализация (с 1980-х годов — с развитием глобальных сетей производства, финансирования и информации).

Глобализация приводит к стиранию национальных границ. В этом контексте следует отметить труд К.Омаэ «Конец национального государства. Восход региональных экономик», где он утверждает, что государства не только теряют способность контролировать обменный курс и защищать свои валюты, но и более не осуществляют реальную экономическую деятельность, не являясь главными действующими лицами в мировой экономике. В подтверждение он опирается на свои выводы в отношении четырех факторов, которые называет «четыре **И**».

Первое «**И**» — это **инвестиции**, которые более не являются географически лимитированными и, пересекая границы, приходят туда, где существуют наиболее привлекательные инвестиционные возможности. Если десять лет назад, пишет автор, поток трансграничных фондов в основном осуществлялся от правительства к правительству или от многосторонней финансовой организации, то в настоящее время инвестиции в подавляющем большинстве являются частными и исключают вовлечение правительств.

Второе «**И**» — **индустрия** в своей ориентации также становится более глобальной. Современные многонациональные корпорации руководствуются не интересами государства, а привлекательностью рынков и способствуют передаче технологий и управленческих ноу-хау.

---

[10] *Philippe Moreau Defarges*. La mondialisation. Presses Universitaires de France, 1997.

[11] http://oecdmoscow.9.com1.ru/oecd_about.html

Третье **«И» — информационные** технологии, которые дают возможность компаниям действовать в различных частях света без необходимости строительства системы бизнеса в каждой стране, где они представлены.

Четвертое **«И» — индивидуальные** потребители, которые стали более глобальными в своей ориентации и хотят иметь нужную продукцию, не зависимо от того, где она производится.

По мнению К.Омаэ, передвижения четырех «**И**» упраздняют роль государства, а ограничения для принятия глобальных решений начинают соответствовать не его границам, а географическим образованьям — например, Гонконгу и прилегающей к нему части Южного Китая, региону Кансай вокруг Токио, или Каталонии, то есть тем регионам, где процветают реальные рынки. Автор называет эти образованья «региональными государствами». Они, по сути, являются естественными экономическими зонами высоких технологий в «мире без границ». К ним он относит Северную Италию, Баден-Вюртемберг, Силиконовую долину и зону Залива в Калифорнии, треугольник Сингапур — Джохор (южный штат Малайзии) и соседние острова Индонезии, г.Пусан (на юге Кореи) и др.[12]

Таким образом, можно говорить о процессе регионализации не как об антагонисте глобализации, а как о ее составной части.

Особый вклад в интеллектуальные дебаты конца XX века внесли работы известного американского ученого Ф.Фукуямы, объявившего конец конфронтации между коммунизмом и западной либеральной демократией «концом истории». Острую полемику, особенно после терактов 11 сентября 2001 г., вызвало утверждение профессора Гарвардского университета С.Хантингтона о «столкновении цивилизаций», который еще в 1993 г. отметил, что международные отношения в период глобализации не подчиняются традиционному разделению между богатыми и бедными странами, а подчиняются культурной парадигме.

В силу этого он считает, что отныне определять основные линии раздела мировой политики будут несколько групп цивилизаций. По его мнению, китайское, индусское, исламское, славянско-православное, западное, японское, латиноамериканское и африканское сообщества формируют наиболее распространенные культурные сферы, которые служат пониманию источников конфликта и напряженности в мире,

[12] *Kenichi Ohmae*. The End of the Nation State. The Rise of Regional Economies. The Free Press, 1995.

где религиозная и историческая принадлежность стала центральным фактором международных отношений[13] .

Известный гарвардский ученый С. Хоффман полагает, что в мире происходит **«столкновение глобализаций»**, поскольку глобализация, по его мнению, имеет три формы.

Первая — это **экономическая**, которая является результатом революции в технологиях, информации, торговле, иностранных инвестициях и международном бизнесе. Специализация и интеграция компаний дала возможность увеличивать совокупное богатство, однако не обеспечивает социальную справедливость.

Вторая — это **культурная** глобализация, которая вырастает из технологической революции и экономической глобализации, стимулирующих передвижение культурных товаров. В культурной глобализации происходит столкновение между униформизацией (американизацией) и движением за культурное разнообразие (как реакцию против единообразия), выражающееся в возрождении местных обычаев, языков и иных национальных атрибутов.

Третья – это **политическая** глобализация, как результирующая от первых двух типов. Она характеризуется доминированием США и их политических институтов, широким спектром международных и региональных организаций, а также сетью неправительственных структур.

Автор считает, что многие из этих организаций испытывают недостаток демократической ответственности, власти и авторитета и выделяет следующие три наиболее важных фактора влияния глобализации на мировую политику.

Первый — **институциональный**. Многие страны неохотно воспринимают ограничение их суверенитета в пользу ООН, власть которой в последнее время нередко проявляется лишь теоретически. Чем чаще страны испытывают на себе негативные последствия глобализации, не говоря о таких явлениях, как «гуманитарная интервенция», тем больше они держатся за то, что у них еще осталось.

Второй – **национальный**. Глобализация не оспаривает национальной основы гражданства, т.к. мир, объединенный в сфере высоких технологий, до сих пор не обладает коллективным сознанием или коллективной солидарностью.

Третий — **угроза терроризма**, т.к. глобализация, снижая различные барьеры, может способствовать распространению конфликтов и тер-

[13] *Samuel P.Huntington*. The Clash of Civilizations? // Foreign Affairs. № 3. 1993.

роризма[14], что в современных условиях приобретает особую актуальность (подробнее в главе 5).

Характерно, что в этом контексте, наряду с позитивными факторами глобализации, о ее негативных аспектах рассуждает в своей книге Д.Сорос. Во-первых, считает он, немало людей испытали удары глобализации без поддержки системы социальной защиты, многие были маргинализированы глобальными рынками. Во-вторых, глобализация стала причиной неправильного распределения между частными и общественными благами (в т.ч. и в проблеме сохранения мира). В-третьих, глобальные финансовые рынки склонны к кризисам (азиатский кризис 1997 г. тому подтверждение). Политические процессы, отмечает он, менее эффективны, чем рыночные механизмы, но мы ничего не можем сделать без них. Критикуя глобальную капиталистическую систему, Сорос призывает к установлению «открытого общества» как необходимого дополнения к экспансии рынков[15].

Американский экономист, лауреат Нобелевской премии 2001 г. в области экономики Д.Стиглиц отмечает, что глобализация может быть силой, направленной на благо. Однако для миллионов людей эта сила не действует, поскольку они потеряли свою работу, а их жизнь стала менее безопасной [16].

Известный экономист, профессор Колумбийского университета Дж.Бхагвати критиков глобализации делит на две категории: непримиримых врагов рыночного капитализма и здравомыслящих, но плохо информированных людей. В качестве аргумента за глобализацию автор приводит пример Индии, которая в последние два десятилетия в условиях открытой экономики снизила уровень бедности с 55 до 26 процентов[17].

1.1.2. Инфономика

Процессы глобализации стимулируются бурным развитием так называемой «новой экономики» («new economy»), основанной на достижениях информационно-технологической революции. Действительно, предоставив уникальные возможности в области передвижения капитала, товаров и услуг, ИКТ стали основой формирования

---

[14] *Stanley Hoffman*. The Clash of Globalizations. // Foreign Affairs. July/August 2002. P. 104–115.

[15] George Soros on Globalization. Oxford, 2002.

[16] *Joseph E.Stiglitz*. Globalization and Its Discontents. London, 2002.

[17] *Jagdish N.Bhagwati*. In Defence of Globalisation. New York, 2004.

так называемой новой экономики (инфономики, киберэкономики). Известный российский исследователь проблематики информационного общества В.Иноземцев использует термин «экономика знаний»[18].

В этом контексте появился термин «глобальная сетевая экономика», который определяется как среда, где компания или индивид, находящиеся в любой точке экономической системы, могут с меньшими затратами контактировать с любой другой компанией или индивидом по поводу совместной работы, для осуществления торговли или обмена идеями. Разворачивающийся прогресс в формировании и расширении масштабов сетевой экономики обусловлен, во-первых, быстрым распространением ИКТ, а также постоянным снижением цен на их приобретение и использование, что повышает их доступность. Во-вторых, наблюдается значительное перемещение различных видов социально-экономической деятельности в электронную среду, которая уже сегодня представляет тысячи видов бизнеса[19]. При этом следует отметить, что здесь каждый может успешно конкурировать даже с общепризнанными гигантами, поскольку компьютерная экономика предоставляет уникальные возможности противостоять монополии и большим фирмам.

Существенные изменения вследствие внедрения ИКТ происходят в следующих трех экономических институтах: торговле, финансах и трудовых отношениях. Электронная коммерция на сегодня является бурно развивающейся отраслью бизнеса. Так, по оценкам компании eMarketer, доходы от электронной коммерции в Европе в 2004 г. составили около 180 млрд. долларов[20].

Эксперты Forrester Research ожидают, что рост онлайновых продаж в США в 2005 г. составит 23% и общий объем онлайновой торговли, исключая путешествия, выйдет на уровень 109 млрд. долл. Онлайновая торговля пока составила 4,6% от общего объема розничных продаж в 2004 г., и ожидается 5,5% в 2005 г. Но ежегодный рост объемов онлайновой торговли в США существенно превышает общие темпы роста розничных продаж, которые растут на 7% в год[21].

---

[18] *Иноземцев В.* Парадоксы постиндустриальной экономики (инвестиции, производительность и хозяйственный рост в 90-е годы) // Мировая экономика и международные отношения. 2000. № 3. С. 3.

[19] Encyclopedia of the New Economy. — http://www.hotwired.com/special/ene/

[20] http://www.e-commerce.ru/

[21] Chicago Tribune. 24.05.2005.

По данным компании comScore, на второе место в мире после США по относительной величине покупающих в Сети поднялась Южная Корея, на третье – Германия[22].

Использование Интернет-технологий несет в себе расширение возможностей координации предпринимательской деятельности, позволяя при минимальных финансовых затратах и отсутствии инфраструктурных барьеров глобально увеличить сеть сбыта продукции. Сегодня компании обладают возможностью проводить видеоконференции и виртуальные презентации, обеспечивающие наибольший охват аудитории; создавать на WWW свои «витрины», где потенциальные покупатели могут не только получить полную информацию о компании, предоставляемых ею услугах и продукции, но и высказать по этому поводу свое мнение. Это, в свою очередь, позволяет компаниям налаживать обратную связь с клиентами, выявлять наиболее популярные услуги и товары и в соответствии с этим координировать свою деятельность. И, наконец, приемлемые затраты на подключение к сети Интернет практически из любой точки планеты сделали возможным уменьшение ограничивающих географических факторов совместной предпринимательской деятельности. Наличие же различных электронных платежных систем предоставило возможность выигрывать на, пожалуй, самом главном в бизнесе — времени.

Сегодня практически все банки ведут свою деятельность через Интернет. Спрос на подобные предложения неуклонно растет. К примеру, по данным отчета Ассоциации канадских банкиров, количество канадцев, пользующихся услугами онлайновых банков, увеличилось почти вдвое за последние два года. Исследование агентства Wahlen показало, что в Германии на сегодняшний день 45% пользователей Сети ведут свои банковские счета через Интернет[23].

ИКТ создают благоприятную почву для развития дистанционных трудовых отношений, называемых теле- или удаленной работой. Если в 1997 г. в Европе численность телерабочих составляла более 2 млн человек, а в США — около 11,1 млн, то в 2003 г. — около 20 % рабочей силы пользовалось теледоступом[24].

ИКТ несут в себе значительные перемены в политической жизни социума. Во-первых, появляется возможность оперативного доступа максимального числа людей к текстам законопроектов еще на стадии их предварительной разработки. Во-вторых, принципиальное ново-

[22] http://e-commerce.ru/analytics/statistics/issue11/stat62.html

[23] http://e-commerce.ru/analytics/statistics/issue9/stat54.html

[24] Status Report on Telework. - http://www.eto.org.uk/twork/tw97eto/

введение заключается в возможности каждого гражданина с относительно минимальными затратами обратиться к неограниченной по своему составу аудитории и высказать по тому или иному вопросу свое мнение. Наиболее полно весь спектр таких возможностей реализуется в так называемом «E-Government» — электронном правительстве (подробнее – в главе 3).

Сегодня практически все государственные структуры имеют свои «страницы» в Интернете, что, в конечном итоге, способствует совершенствованию демократических процедур, повышению политической активности населения, установлению более эффективного диалога государства с бизнесом и общественностью. Ускоряющееся развитие и распространение ИКТ и систем, связанных между собой и пересекающих традиционные национальные, политические и экономические границы, привели к вынужденному изменению направления политической мысли. Характерно, что общественно-политический лексикон за последние годы обогатился такими понятиями, как «электронное правительство», «электронное гражданство», «киберполитика», «кибердемократия», «компьютероопосредованная политическая коммуникация» и рядом других[25].

Информационно-технологическая революция определяет движение к совершенно новому типу общества — информационному, или, как его еще называют, обществу знания. Одной из основополагающих характеристик этого общества является его глобальный характер. В процессе его формирования постепенно стираются границы между странами и людьми, радикально меняется структура мировой экономики, значительно более динамичным и конкурентным становится рынок. Информация и знания становятся одним из стратегических ресурсов государства, масштабы использования которого стали сопоставимы с использованием традиционных ресурсов, а доступ к ним — одним из основных факторов социально-экономического развития. В связи с этим к числу важнейших задач каждого государства относятся формирование и развитие информационной инфрастуктуры и интеграция в глобальное информационное общество. Решение этих задач становится сегодня необходимым условием устойчивого развития государства и его полноценного вхождения в мировое сообщество.

Впервые на высшем уровне постулируемый тезис нашел свое отражение в Окинавской Хартии глобального информационного обще-

[25] *Чернов А.А.* Становление глобального информационного общества: проблемы и перспективы. М.: Дашков и К°, 2003. С. 6.

ства, принятой лидерами «восьмерки» 22 июля 2000 г.: «Информационно-коммуникационные технологии являются одним из наиболее важных факторов, влияющих на формирование общества XXI века»[26]. Наиболее глубоко эта проблема представлена в документах Всемирной встречи в верхах по глобальному информационному обществу, первый этап которой состоялся в Женеве[27] в декабре 2003 г., а второй — в ноябре 2005 г. в Тунисе (подробнее в главе 2).

Действительно, наступил принципиально новый этап в развитии процессов обмена информацией. Интенсивное внедрение и переплетение современных компьютерных, теле- и радиовещательных технологий и коммуникационных служб, бурное распространение локальных и глобальных сетей создают принципиально новое качество трансграничного информационного обмена и инструментария воздействия на массовое сознание, усиливая значение социально-психологических и культурно-информационных аспектов глобализации.

Вместе с тем современные информационные технологии, все глубже проникая во все сферы общественной жизни, генерируют не только новые возможности в решении различных накопившихся проблем, но и принципиально новые вызовы и угрозы. Среди них наметившийся цифровой разрыв как между странами, так и внутри них, соблюдение свободы слова, защита интересов этнических меньшинств и подрастающего поколения, сохранение национального языка и культурного наследия, противостояние культурной экспансии других стран, охрана интеллектуальной собственности, борьба с компьютерными и высокотехнологичными преступлениями и, наконец, разработка некоторыми странами (по некоторым оценкам таких стран свыше 100) концепций информационных войн с применением принципиально нового оружия – информационного (подробнее в главе 5). В силу этого в России была разработана и утверждена Президентом России В.В.Путиным 9 сентября 2000 г. Доктрина информационной безопасности[28].

В качестве резюме к соотношению процессов глобализации и развития ИКТ представляется оправданным согласиться с мнением одного из ведущих экспертов данной проблемы, известного социолога, исследователя проблематики информационной эпохи профессора Калифорнийского университета М.Кастелса. Он рассматривает гло-

---

[26] Окинавская Хартия глобального информационного общества // Дипломатический вестник. 2000. № 8. С. 52.

[27] http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!MSW-R.doc

[28] http://www.scrf.gov.ru/Documents/Decree/2000/09-09.html

бализацию в качестве новой экономики, для которой свойственно определяющее влияние ИКТ и их реализация через сетевые структуры[29].

1.1.3. Динамика развития ИКТ

Лауреат Нобелевской премии по физике 2000 года Ж.И.Алферов считает ИКТ самой динамичной отраслью экономики в мире, подтверждая данный тезис следующими аргументами[30]. Темпы ее роста в три раза выше темпов ростов ВВП. В отрасли производится продукции на 15 триллионов долларов. Среднемировой срок окупаемости вложений — 2-3 года (1 вложенный доллар США дает 100 долларов в конечном продукте). Одно рабочее место в электронике дает четыре в других отраслях. Один килограмм изделий микроэлектроники по стоимости эквивалентен стоимости 110 тонн нефти. Если сегодня посмотреть на то, как поделены мировые рынки по объемам производства ИКТ, то это примерно четыре равные часта — США, Япония, Юго-Восточная Азия (за исключением Японии) и Европа. Стремительно приближается к ним Китай, который построит у себя более половины из намеченных 13 новейших предприятий в мире по производству 300-мм кремниевых подложек для интегральных схем (на сегодняшний день их насчитывается уже 30).

Поразительны темпы развития ИКТ: в 1959 г. первая интегральная схема — два транзистора, РЦ-цепочка, в 2000 г. — 43 миллиона транзисторов, а к 2014 г. ожидается 4, 3 миллиарда транзисторов на одной интегральной схеме. Стоимость одного мегагерца в микропроцессорах в 1970 г. составляла 7, 6 тыс. долларов, а в 2000 г. — 16 центов.

Еще один пример. Пятьдесят лет тому назад для того, чтобы переслать 30 страниц текста на расстояние 5 тысяч км потребовалось бы примерно десять дней и стоило бы это около 30 долларов за услуги почтовой связи. Двадцать лет тому назад по факсу это заняло бы примерно час, и стоило бы 50 долларов. Сегодня, если говорить о самых лучших сетях передачи данных, на это потребуется не более 3 секунд и стоимость составит около 3 центов.

Правительство Японии официально объявило о том, что в апреле 2006 г. начнется сборка суперкомпьютера, вычислительная мощность

---

[29] *Кастелс М.* Информационная эпоха: экономика, общество, и культура/ Под ред. О.И.Шкаратана. М.: ГУ ВШЭ, 2000.

[30] См. *Алферов Ж.И.* Отрасль отчаяния, отрасль надежды // Экономическая философская газета. 08.06.2004. № 022

которого достигнет 10 квадрильонов (10^{15}) операций в секунду, или 10 петафлоп[31]. Новый японский кластер будет в 73 раза производительнее нынешнего лидера списка Top500 — американской системы Blue Gene/L от IBM.

Тендер на создание суперкомпьютера выиграли компании NEC и Hitachi, а научную базу подготовят университеты г. Токио и острова Кюсю. Новый суперкомпьютер позволит японским ученым более точно моделировать действие лекарственных препаратов, создавать модели зарождения Вселенной, делать достоверные прогнозы погоды и проч.

Всего в разработку новой системы будет инвестировано от 80 до 100 млрд йен ($714–893 млн). Если бюджет на 2006 год будет принят, то проект создания суперкомпьютера нового поколения будет завершен в 2010 финансовом году, который заканчивается в марте 2011 г.

Суперкомпьютер Blue Gene, созданный в IBM, установлен и работает в Ливерморской национальной лаборатории им. Лоуренса министерства энергетики США. Ему принадлежит нынешний мировой рекорд производительности — 135,3 трлн операций в секунду (135,3 терафлоп). До этого в течение трех лет (с июня 2002 года) мировым лидером в области суперкомпьютерных вычислений являлся японский кластер Earth Simulator, построенный из компьютеров NEC SX-6, производительность которого достигала 35,86 терафлоп. В настоящее время Earth Simulator находится на четвертом месте — он уступает двум системам Blue Gene от IBM и суперкомпьютеру Columbia от компании SGI, установленному в НАСА и работающему на базе процессоров Intel Itanium 2.

Все свои рекорды Blue Gene/L поставил, находясь в недостроенном состоянии. Завершить сборку Blue Gene планируется уже в этом году. Предполагается, что это позволит суперкомпьютеру достичь быстродействия в 360 терафлоп. С момента появления в 1976 г. в Лос-Аламосской лаборатории первого суперкомпьютера Cray-1, выполнявшего 80 млн операций в секунду, этот показатель вырос в 500 тыс. раз. Кроме того, Blue Gene/L требуется в 15 раз меньше энергии, чем первым суперкомпьютерам.

В своей финальной конфигурации компьютер Blue Gene позволит ученым, в частности, изучать методами математического моделирования различные аспекты безопасности, защищенности и надежности ядерного арсенала США без проведения для этого ядерных испытаний. Но «военная» тема — не единственная. Использование суперкомпьютеров уже

[31] http://www.cnews.ru/news/top/index.shtml?2005/07/26/183160

позволило ученым существенно продвинуться в понимании структуры белков, климатических процессов, разрушительных стихийных феноменов — таких, как цунами.

Лозаннский политехнический институт приобрел у компании IBM суперкомпьютер Blue Gene/L для проекта **по моделированию человеческого мозга.** Сотрудники исследовательских подразделений IBM будут принимать непосредственное участие в разработках под кодовым названием Blue Brain. С помощью такого компьютера исследователи надеются пролить свет на главные загадки человеческого мозга – познание, память и, возможно, само сознание.

По словам директора Отделения мозга и разума при Лозаннском политехническом институте Анри Маркрама, впервые человечество сможет моделировать те электрические импульсы, которыми мозг кодирует информацию об окружающем мире. Как заявил New Scientist Чарльз Пек, ведущий исследователь IBM, занятый в проекте, до сих пор создание подобного компьютера было невозможно по двум причинам: во-первых, у науки не было достаточных данных о том, как между собой связаны нейроны в мозге, во-вторых, отсутствовали достаточные вычислительные мощности.

Захватывающие перспективы для ИКТ создает **нанотехнология**. Как сообщает журнал «Nanoscience and Nanotechnology»[32], ученые Ашутош Тивари (Ashutosh Tiwari) и Ягдиш Нараян (Jagdish Narayan) из университета Северной Каролины смогли создать наноточки (квантовые точки) диаметром около 5 нанометров, что на порядок меньше, чем удавалось ранее. Каждая такая наноточка представляет собой локальное вкрапление (кластер), состоящее из нескольких сотен атомов никеля, и может иметь одно из двух возможных магнитных состояний. Это позволяет использовать их для хранения информации, присваивая его состояниям одно из двух возможных значений — «0» или «1». В обычных компьютерных винчестерах информация хранится на дисках, покрытых магнитным материалом, и для предотвращения нежелательной интерференции между областями, хранящими отдельные биты информации, необходимо, чтобы они располагались на достаточном удалении друг от друга. Наноточки можно «упаковывать» намного плотнее, поскольку они представляют собой дискретные образования и структурно не связаны друг с другом.

Методика создания таких наноточек следующая: с помощью импульсного лазера никель нагревается до образования плазмы.

[32] http://www.cnews.ru/newtop/index.shtml?2004/09/09/163259

В этом состоянии он образует на подложках из двух различных материалов — оксида алюминия и нитрата олова и титана — наноточки одинакового размера. При этом их плотность (число точек на единицу площади) такова, что, теоретически, позволяет записать до 5 терабайт данных на площади размером со стандартную почтовую марку. По мнению Тивари, теперь ученым необходимо найти способ, позволяющий интегрировать эти наноточки в кремниевых чипах.

Еще более поразительные перспективы развития ИКТ связаны с использованием ДНК. Известно, что молекулы ДНК являются носителем генетической информации. Они обладают множеством уникальных свойств, среди которых есть и способность к самосборке молекул ДНК по определенному шаблону[33].

В данном случае ДНК используют для создания матрицы — своеобразного каркаса, с помощью которого можно укладывать «строительные блоки», состоящие из различных металлов или органических молекул. Эти «строительные блоки» могут сохранять электрические или магнитные заряды и, значит, могут играть роль устройств хранения информации. Для создания матрицы используется искусственная ДНК, а ее способность к самосборке в виде определенной пространственной конструкции регулируют с помощью подбора компонентов и внешних условий. Присоединение блоков регулируется также с помощью молекулярных свойств фрагментов ДНК, которые обладают высокой избирательностью.

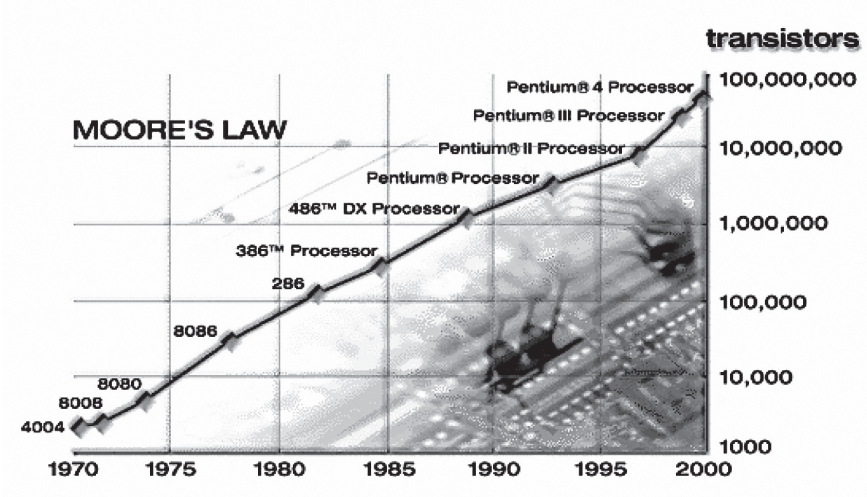
Благодаря сверхмалым размерам электронных компонентов (порядка 1 нм) и малому расстоянию между ними, которое может достигать одной трети нанометра, плотность хранения информации в этом случае может увеличиться в 1000 раз по сравнению с нынешними наиболее совершенными системами. Многократно возрастет и быстродействие из-за малых расстояний между элементарными ячейками хранения информации.

Ученым из США (Миннесота) удалось получить первые образцы наноэлектронных схем, созданные с помощью биомолекул. В частности, им удалось уложить в регулярном порядке микрошарики из золота диаметром 1,4 нм. Данный метод способен привести в скором будущем к полному отказу от используемых ныне литографических процессов и переходу на нанотехнологию.

В целом динамику развития ИКТ удалось сформулировать инженеру компании Intel Муру, который дал свое имя соответствующему

[33] http://www.cnews.ru/newtop/index.shtml?2004/12/22/170917

закону. Закон Мура: темпы изменений ИКТ значительно опережают темпы изменений прежних технологий. Под воздействием факторов, лежащих в основе этого закона (удвоение числа транзисторов на квадратный дюйм каждые 18 месяцев), инновации в ИКТ сменяют друг друга с огромной скоростью. Ниже приводится график, подтверждающий закон Мура[34].



Резюмируя данный параграф, можно со всей определенностью сказать, что **ИКТ являются не только самым динамично развивающимся сегментом мировой экономики, но и — в силу своих функциональных характеристик — локомотивом и нервом глобализации**.

1.1.4.Основные этапы создания Интернета

Началом компьютерной эры принято считать 1946 г. Тогда в США был создан компьютер ЭНИАК, который имел 19 тысяч электронных ламп и весил около 30 тонн. ЭНИАК применялся для особо важных и секретных вычислений в военной сфере (при этом его мощность значительно уступала современным бытовым компьютерам на базе процессора «Pentium») и был цифровым, а не аналоговым устройством.

[34] http://www.intel.com/research/silicon/mooreslaw.htm

То есть он представлял числа не в виде какой-то измеряемой величины, например напряжения тока, а кодировал их цифрами в десятичной системе от 0 до 9.

Достаточно высокое быстродействие достигалось благодаря тому, что ЭНИАК был чисто электронным устройством, имевшим механические детали только в системе ввода-вывода. ЭНИАК мог выполнять самые разные вычисления в зависимости от заданной программы, которая вводилась переключателями на панели управления. Современная архитектура компьютера сформировалась в преемнике ЭНИАКа, получившем название ЭДВАК, в котором программы хранились в той же электронной памяти, что и результаты вычислений. Кроме того, ЭДВАК работал в двоичной системе, используя две цифры — 0 и 1, что значительно упрощало электрические схемы (аналогично азбуке Морзе: точка, тире и только один ключ).

Единица информации, которая соответствует выбору между 0 и 1, т.е. между положением «включено» и «выключено», получила название ***бит***. Буквы кодируются в электронной памяти, как правило, в виде 8-битовой комбинации, получившей название ***байт***. Байт соответствует выбору из 256 различных возможностей. Производные величины — килобит, килобайт, мегабит, мегабайт и т.д. — имеют коэффициент 1024 — достаточно круглое число в двоичной системе.

Компьютеры стремительно развивались, дешевели и уменьшались в размерах, т.к. электронные лампы в них сменились сначала транзисторами, затем — интегральными схемами (чипами). При этом каждые полтора-два года происходило удвоение их основных рабочих параметров.

Развитие компьютеров позволило выполнять им, наряду со сложными вычислениями, и функции хранилища данных, заменяя бумажные картотеки. Появление в 70-е годы персональных компьютеров принципиально изменило вначале работу в полиграфии, а затем и все делопроизводство. Наиболее распространенной функцией компьютера стала функция «умной» пишущей машинки.

Запуск в 1957 г. первого советского искусственного спутника Земли был воспринят в США как вызов. В ответ было создано Агентство по новейшим исследованиям (ARPA) при Министерстве обороны США, первым проектом которого стал американский спутник, а с начала 60-х годов — военное использование компьютерных технологий.

С учетом высокой стоимости крупные университеты могли себе позволить приобрести не более 1-2 больших компьютеров. Для работы на них специалисты записывались заранее, пока, наконец, не появилась идея соединить между собой компьютеры разных университетов,

чтобы сделать возможным удаленное использование любого свободного в данный момент компьютера. 2 сентября 1969 г. в лаборатории Калифорнийского университета профессор Лен Клейнрок, которому помогали студенты Стивен Крокер и широко известный ныне Винтон Серф, соединили два компьютера пятиметровым кабелем и отправили по нему некий набор данных[35]. Считается, что это была первая передача информации по компьютерной сети. Именно из этого эксперимента появилась сеть ARPANET, а затем и современный Интернет[36].

С начала 70-х годов от ARPA начинают требовать прямой военной отдачи, и к названию Агентства добавляется буква «D» (первая буква слова «Defense» — оборонное), и учреждение получает обозначение DARPA. Иными словами, ARPANET был разработан при самом непосредственном участии Пентагона, а также лучших умов американских научных центров и университетов в годы «холодной войны». Интернет задумывался как действенный механизм быстрого электронного реагирования на любую опасность (в том числе ядерную) и создания иммунитета от нее, как система срочной связи, объединяющей американские передовые военные базы и базы электронного слежения.

В 1972 г. ARPANET уже соединяла 23 компьютера, в этом же году была написана первая программа для обмена электронной почтой по сети. Вскоре обнаружилось, что сеть чаще используется не по своему основному назначению — для вычислений на удаленном компьютере, — а для обмена сообщениями, т.е. электронной почты.

В середине 70-х годов для ARPANET были разработаны новые стандарты передачи данных, которые позволяли объединять между собой сети произвольной архитектуры. **Тогда же вошло в лексикон и слово Интернет**. Именно эти стандарты, получившие название протокола TCP/IP, заложили основу для роста глобальной компьютерной сети путем объединения уже существующих сетей. В 1983 г. сеть ARPANET перешла на новый протокол и разделилась на две независимые сети — военную и образовательную. К этому времени сеть объединяла более тысячи компьютеров, в том числе в Европе и на Гавайских островах. С этого момента американское военное ведомство уже не играло прежней роли в развитии Интернета, хотя некоторое время еще продол-

[35] http://www.webplanet.ru/news/internet/2004/8/30/35years.html

[36] http://www.cybergeography.org/atlas/historical.html

жало финансировать образовательную часть ARPANET. Интернет оставался преимущественно университетской сетью до начала 90-х годов, когда насчитывал уже около 60 тысяч соединенных компьютеров.

Стремительное развитие Интернета началось в 1992 г., когда была изобретена новая служба, получившая название «Всемирная паутина» (World Wide Web, или WWW, или просто «веб», то есть «паутина»). Паутина позволяла любому пользователю публиковать свои текстовые и графические материалы, связывая их с публикациями других авторов и предоставляя удобную систему перемещения от документа к документу. Таким образом, Интернет стал превращаться из средства переписки и обмена файлами в гигантское хранилище информации. К концу 1992 г. Интернет насчитывал уже более миллиона соединенных компьютеров.

В этот же период Интернет проник в Россию, когда ряд университетов и НИИ приступил к построению своих компьютерных сетей и получил доступ к зарубежным каналам связи. Так, на базе Института атомной энергии им.Курчатова сложились крупнейшие коммерческие компании, предоставляющие услуги по подключению к Интернету — «Релком» и (впоследствии отделившийся от него) «Демос», а также Российский институт развития общественных сетей (РОСНИИРОС), бывший до 2004 г. головной организацией, координировавшей развитие российской зоны Интернета.

В 1993 г. достаточно мощный импульс развитию Интернета в России придала «Телекоммуникационная программа» Международного научного фонда, финансируемая Д.Соросом, который полагал, что распространение Интернета в бывших социалистических странах поможет им преодолеть сложившуюся информационную изоляцию. Одновременно быстрыми темпами развивались сети провайдеров — коммерческих поставщиков услуг Интернета как акционерные общества с чисто российским или смешанным капиталом. Вначале они ориентировались на подключение банков, госучреждений, СМИ, а затем они все шире стали обслуживать и частных пользователей.

По оценкам Региональной общественной организации «Центр Интернет-технологий» (РОЦИТ), в начале 2005 г. в России было около 18 миллионов пользователей Интернета, больше половины которых проживает за пределами Москвы (подробнее в главе 4). По доле от всего населения 13% — это примерно соответствует уровню охвата Интернетом стран Латинской Америки, в несколько раз меньше, чем в США, Канаде, Австралии, Великобритании, Скандинавских стра-

нах, Японии, Южной Корее, хотя и выше, чем в Индии, Китае и африканских странах[37].

Аудитория пользователей чрезвычайно разнообразна и по способу подключения. Оно осуществляется через модемы или локальные сети с персональных компьютеров, в том числе с карманных (PDA), телевизоров с поддержкой веб-услуг, мобильных телефонов, коммуникаторов и т.д. Данные оценки достаточно условны, поскольку в Интернете нет центрального органа, который бы регистрировал всех новых пользователей или новые компьютеры. Данный феномен неразрывно связан с появлением глобальных компьютерных сетей, и в первую очередь Интернета, которые неизмеримо увеличили мощность и информационные возможности отдельных компьютеров. Их появление и начавшаяся по всему миру либерализация рынка, следствием которой стало соответствующее снижение стоимости коммуникационных услуг, — два, пожалуй, основных фактора, которые сыграли определяющую роль в развитии информационной сферы, усиления ее социального аспекта. Снижение цен на компьютеры и связь сделали их доступными для широких масс людей, а не только для бизнеса и государственных учреждений, что, в свою очередь, оказало решающее воздействие на информационную индустрию, у которой появились миллионы новых потребителей и обширные рынки сбыта. Согласно широко известным данным, **чтобы достичь аудитории в 50 млн человек, радио понадобилось 30 лет, телевидению — 13 лет, а Интернету — всего 4 года.**

Бурное развитие Интернета как ядра становления информационного общества породило ряд системных проблем, которые рассматриваются в различных международных организациях и структурах.

С учетом этого обстоятельства, а также объективного характера процессов информационной глобализации и новых вызовов, которые она несет, требуется существенное и оперативное изменение повестки дня мировой политики и международных организаций. Об особой актуальности данной проблемы справедливо ставит вопрос целый ряд экспертов и дипломатов как российских, так и зарубежных[38].

В первую очередь это касается ООН и ее структур, которые, в целом немало делая по поиску адекватных ответов на данные вызовы, тем не менее не в состоянии в нынешнем формате полноценно реагировать и продвигать необходимые решения. Подробнее данная проблема рассматривается в следующей главе.

---

[37] http://www.nua.ie/surveys/how_many_online/index.html

[38] См. *Арыстанбекова А.* Глобализация. Объективная логика и новые вызовы // Международная жизнь. 2004. № 4–5.

1.2. Базовые понятия и сущностные черты глобального информационного общества

Бурное развитие ИКТ, резкое усиление их влияния практически на все аспекты экономических, социальных и культурных отношений мирового и национальных социумов, вызвали необходимость переосмысления всей парадигмы социума, который в последнее время исследователями определяется как «глобальное информационное общество».

1.2.1. Эволюция понятия «информационное общество»

На первый взгляд «информационной», как и «постиндустриальной», может быть не общество, а экономика. Тем не менее это понятие дефакто обрело статус официального, поскольку широко используется не только в СМИ и политологической литературе, но и в документах государственных и международных структур. Термин **«информационное общество»**[39] используется в них для обозначения цели, которая может быть достигнута в ходе повсеместного внедрения ИКТ. Считается, что таким образом повсюду в мире может быть обеспечен устойчивый экономический рост, повышено общественное благосостояние, укреплено социальное согласие, реализован потенциал большинства стран мира и, в конечном счете, обеспечены транспарентное и ответственное управление в мировом сообществе, а также международная стабильность.

Впервые понятие «информационное общество» появилось во второй половине 1960-х годов, которое приписывается профессору Токийского технологического института Ю. Хаяши. Основные его характеристики были определены в отчетах, представленных японскому правительству рядом организаций: Агентством экономического планирования, Институтом разработки использования компьютеров, Советом по структуре промышленности. Показательны сами названия документов: «Японское информационное общество: темы и подходы» (1969 г.), «Контуры политики содействия информатизации японского общества» (1969 г.), «План информационного общества» (1971 г.)[40]. В отчетах высокоиндустриальное

[39] Другие «информационные» термины и определения приводятся в глоссарии.

[40] *Алексеева И.Ю.* Возникновение идеологии информационного общества // Информационное общество. 1999. № 1. С. 30—35.

общество определялось как такое, где развитие компьютеризации предоставит людям доступ к надежным источникам информации и избавит их от рутинной работы, обеспечив высокий уровень автоматизации производства. При этом существенные изменения коснутся непосредственно самого производства, в результате которых его продукт станет более «информационно емким», что приведет к значительному увеличению доли инноваций, дизайна и маркетинга в его стоимости. Производство информационного продукта, а не продукта материального, по мнению авторов, будет движущей силой образования и развития общества.

Очень быстро постиндустриальная проблематика становится одной из ведущих в западной политологии. Основной акцент в исследованиях этого времени ставится в основном на необходимости совершенствования средств получения, обработки и распространения информации и результатах их использования в экономической сфере. Обусловлено это было бурным развитием и конвергенцией ИКТ, повлекшими за собой революционные изменения на мировом рынке. Гуманитарные аспекты формирования нового общества, в частности социальные проблемы, стали активно изучаться лишь в результате осознания того, что наблюдаемый качественный скачок в развитии информационных технологий породил новую глобальную социальную революцию, ничуть не уступающую революциям прошлого по силе своего воздействия на человеческое общество.

Существенным толчком для дальнейшего развития идей глобального информационного общества послужил выход в 1973 г. книги американского социолога Д. Белла «Грядущее постиндустриальное общество. Опыт социального прогнозирования»[41]. В ней автор разделяет историю человеческого общества на три основные стадии: аграрную, индустриальную и постиндустриальную. Ученый стремился обрисовать контуры постиндустриального общества, во многом отталкиваясь от характеристик индустриальной стадии. Подобно Т. Веблену он трактует индустриальное общество как общество, в котором главной целью ставится производство максимального числа машин и вещей. Существенной чертой постиндустриальной стадии является, по мнению Д. Белла, переход от производства вещей к развитию производства услуг, связанных с образованием, здравоохранением, исследованиями и управлением.

[41] *Bell D.* The Coming of Post-industrial Society. A Venture in Social Forecasting. N.Y.: Basic Books, Inc., 1973.

Важнейшее значение для принятия решений и координации направления изменений приобретает центральная роль теоретического знания. «Любое современное общество живет за счет инноваций и социального контроля за изменениями, — пишет Д. Белл. — Оно пытается предвидеть будущее и осуществлять планирование. Именно изменение в осознании природы инноваций делает решающим теоретическое знание»[42]. Движение в этом направлении будет набирать силу в ходе своего рода соединения науки, техники и экономики. Знание и информацию американский ученый считает не только эффективным катализатором трансформации постиндустриального общества, но и его стратегическим ресурсом.

Указанная книга вызвала всеобщий резонанс и интерес к затронутой в ней проблематике. Начиная с момента ее выхода в свет, появляются многочисленные работы, посвященные осмыслению исторического рубежа, на котором оказалось человечество.

Одна из наиболее интересных и разработанных философских концепций информационного общества принадлежит японскому ученому И. Масуде. Основные принципы и особенности грядущего общества представлены в его книге «Информационное общество как постиндустриальное общество»[43]. Фундаментом нового общества станет, по мнению автора, компьютерная технология, главная функция которой видится им в замещении либо значительном усилении умственного труда человека. Информационно-технологическая революция будет быстро превращаться в новую производственную силу и сделает возможным массовое производство когнитивной и систематизированной информации, новых технологий и знания. Потенциальным рынком станет «граница познанного», возрастет возможность решения насущных проблем и развития сотрудничества. Ведущей отраслью экономики станет интеллектуальное производство, продукция которого будет аккумулироваться и распространяться с помощью новых телекоммуникационных технологий.

Уделяя особое внимание трансформации человеческих ценностей в глобальном информационном обществе, И. Масуда предполагает, что оно будет бесклассовом и бесконфликтным, это будет общество согласия с небольшим правительством и государственным

[42] Ibid. P. 20.

[43] *Masuda Y.* The Information Society as Postindustrial Society. Washington: World Future Soc., 1983.

аппаратом. Он подчеркивает, что **в отличие от индустриального общества, характерной ценностью которого является потребление товаров, информационное общество выдвигает в качестве такой ценности время.**

Известный английский ученый Т. Стоуньер утверждал, что информацию, подобно капиталу, можно накапливать и хранить для будущего использования. В постиндустриальном обществе национальные информационные ресурсы превратятся, как он считает, в самый большой потенциальный источник богатства. В связи с этим следует всеми силами развивать, в первую очередь, новую отрасль экономики — информационную. Промышленность в новом обществе по общим показателям занятости и своей доли в национальном продукте уступит место сфере услуг, которая будет представлять собой преимущественно сбор, обработку и различные виды предоставления требуемой информации[44].

По мере развития электронных СМИ и информационных технологий в научных кругах все более активно ведется дискуссия о функциях и роли информации в жизни общества, тенденциях формирования глобального информационного общества. Особый интерес здесь представляют два имени – Маршалл Маклюэн (Канада) и Элвин Тоффлер (США). Сразу хотелось бы отметить, что подходы, представленные ими в своих исследованиях, получили как положительные, так и далеко не лестные оценки со стороны традиционной науки и общественности в целом.

Отличительной особенностью взглядов М. Маклюэна является то обстоятельство, что ИКТ рассматриваются им в качестве главного фактора, влияющего на формирование социально-экономической основы нового общества. Телекоммуникационные и компьютерные сети сыграют роль своеобразной нервной системы в образовании «глобального объятия», где все оказывается настолько взаимосвязано, что в результате происходит становление «глобальной деревни».

Говоря о перспективах развития средств массовой коммуникации в информационном обществе, Маклюэн неоднократно подчеркивает тенденцию усиления активной роли масс-медиа. Массовая коммуникация как структурно оформившаяся сфера жизни общества видится им в недалеком будущем, с одной стороны, его частью, а с другой — таинственной силой, имеющей над этим обществом все возрастающую власть.

---

[44] Стоуньер Т. Информационное богатство: профиль постиндустриальной экономики // Новая технократическая волна на Западе. М., 1986. С. 335.

Другой теоретик информационного общества Э. Тоффлер предлагает собственную схему исторического процесса. В своей книге «Третья волна» он выделил в истории цивилизации три волны: **первая волна – аграрная (до XVIII века), вторая – индустриальная (до 50-х годов XX века) и третья – постиндустриальная (начиная с 50-х годов).** «Ближайший исторический рубеж так же глубок, как и первая волна изменений, запущенная десять тысяч лет назад путем введения сельского хозяйства, — пишет он. — Вторая волна изменений была вызвана индустриальной революцией. Мы – дети следующей трансформации, третьей волны»[45]. Последняя обозначилась в результате разворачивающейся информационной революции.

Постиндустриальному обществу, на его взгляд, присущи такие черты, как деконцентрация производства и населения, резкий рост информационного обмена, превалирование самоуправленческих политических систем, а также дальнейшая индивидуализация личности при сохранении солидарных отношений между людьми и сообществами.

Традиционным громоздким корпорациям Тоффлер противопоставляет малые экономические формы, среди которых он особенно выделяет индивидуальную деятельность в «электронном коттедже». Последний представляется автору следующим образом: «Радикальные изменения в сфере производства неизбежно повлекут за собой захватывающий дух социальные изменения. Еще при жизни нашего поколения крупнейшие фабрики и учреждения наполовину опустеют и превратятся в складские или жилые помещения. Когда в один прекрасный день мы получим технику, позволяющую в каждом доме оборудовать недорогое рабочее место, оснащенное «умной» печатной машинкой, а может быть, еще и копировальной машиной или компьютерным пультом и телекоммуникационным устройством, то возможности организации работы на дому резко возрастут».

В тот период считалось, что основой формирования информационного общества является развитие ИКТ. Назывался и ряд других признаков:

- информация приобретает глобальный характер;
- на движение информационных потоков уже не оказывают существенного влияния государственные границы и различные барьеры;

[45] *Тоффлер Э.* Третья волна // США — экономика, политика, идеология. 1982. № 7–11.

- попытки ограничить свободное распространение информации наносит вред стране, стремящейся внести такого рода ограничения;
- значительно выросли возможности сбора, обработки, хранения, передачи информации, доступа к ней;
- увеличивается воздействие информации на развитие различных сфер человеческой деятельности;
- углубляется процесс децентрализации общества; происходит переход к новым формам занятости;
- идет процесс формирования новых трудовых ресурсов за счет увеличения количества занятых в информационной индустрии.

Рубеж 1990-х годов можно обозначить как начало нового этапа в развитии идей глобального информационного общества. Прежде всего этот период связан с результатами исследований Питера Дракера и Мануэля Кастельса. П. Дракер, известный американский экономист, один из создателей современной теории менеджмента, принимал участие еще в дискуссиях начала 70-х годов. Однако свой непосредственный вклад в формирование нового облика существующих концепций постиндустриализма он внес позднее в книге «Посткапиталистическое общество»[46]. Ядром концепции Дракера является идея преодоления традиционного капитализма, причем основными признаками происходящего сдвига считаются переход от индустриального хозяйства к экономической системе, основанной на знаниях и информации, преодоление капиталистической частной собственности, формирование новой системы ценностей современного человека и трансформация национального государства под воздействием процессов глобализации. Современная эпоха, по мнению Дракера, представляет собой время радикальной перестройки, когда с развитием новых ИКТ человечество получило реальный шанс преобразовать капиталистическое общество в общество, основанное на знаниях.

М. Кастельс в качестве отправной точки своих размышлений использует глобальную экономику и международные финансовые рынки как основные признаки формирующегося нового миропорядка. Его фундаментальное исследование «Информационная эра: экономика, общество и культура» посвящено развернутому анализу современных тенденций, приводящих к формированию основ общества, которое он назвал «сетевым»[47]. Исходя из того, что информация по своей природе является таким ресурсом, который легче других проникает через

[46] *Дракер П.* Посткапиталистическое общество. СПб., 1999.

[47] *Кастельс М.* Информационная эпоха: экономика, общество и культура. М., 2000.

всевозможные преграды и границы, информационная эра рассматривается им как эпоха глобализации. При этом сетевые структуры становятся одновременно и средством, и результатом глобализации общества. В своей книге автор неоднократно обращает внимание читателя на тот принципиально важный момент, что информация и обмен информацией сопровождали развитие цивилизации на протяжении всей истории человечества и имели особое значение во всех обществах. В то же время зарождающееся новое общество строится таким образом, что сбор, анализ и передача необходимой информации стали «фундаментальными источниками производительности и власти».

За последнее десятилетие к теме ГИО неоднократно обращались и отечественные ученые, которые разработали собственные определения нового общества. Так, известный отечественный исследователь А.И. Ракитов еще в конце 80-годов писал, что переход к информационному обществу предполагает превращение производства и использования услуг и знаний в важнейший продукт социальной деятельности, причем удельный вес знаний будет постоянно возрастать. Главной целью информационного общества является обеспечение правовых и социальных гарантий того, что каждый гражданин общества, находящийся в любом месте и в любое время, сможет получить всю необходимую для решения насущных проблем информацию. По его мнению, основными критериями информационного общества могут служить количество и качество имеющейся в обработке информации, а также ее эффективная передача и переработка. Дополнительным критерием является доступность информации для каждого человека, которая достигается снижением ее стоимости в результате развития и своевременного внедрения новых телекоммуникационных технологий. Залогом успешного функционирования экономики постиндустриального общества станет ее информационный сектор, который выйдет на первые позиции по числу занятых в нем трудящихся[48]. С учетом этого развитие, прежде всего, данного сектора позволит значительно ускорить интеграцию отдельно взятой страны в ГИО.

Другие известные исследователи Д.С.Черешкин и Г.Л.Смолян в разработанном ими подходе к основным признакам нового общества относят:

- формирование единого информационного пространства и углубление процессов информационной и экономической интеграции стран и народов;

[48] *Ракитов А.И.* Наш путь к информационному обществу // Теория и практика общественно-научной информации. М.: ИНИОН, 1989.

- становление и в дальнейшем доминирование в экономике стран, наиболее далеко продвинувшихся на пути к информационному обществу, новых технологических укладов, базирующихся на массовом использовании сетевых информационных технологий, перспективных средств вычислительной техники и телекоммуникаций;
- повышение уровня образования за счет расширения возможностей систем информационного обмена на международном, национальном и региональном уровнях и, соответственно, повышение роли квалификации, профессионализма и способностей к творчеству как основных характеристик услуг труда[49].

Одновременно в концепции особое внимание уделяется вопросам информационной безопасности личности, общества и государства в складывающемся обществе и создания эффективной системы обеспечения прав граждан и социальных институтов на свободное получение, распространение и использование информации.

Известный ученый, академик Н. Моисеев считал, что без свободного доступа всех людей к информации вообще не имеет смысла говорить о построении информационного общества – **«общества коллективного интеллекта планетарного масштаба»**. Однако эта труднейшая социально-политическая проблема, на его взгляд, вряд ли может быть решена в рамках современных «присваивающих» цивилизаций, в которых большая часть людей далеко не всегда готова делиться знаниями. В силу этого необходима смена шкалы ценностей и менталитета[50].

Начиная с 90-х годов, большинство американских и европейских исследователей в этой области стали акцентировать внимание на беспрецедентном ускорении прироста информации. **Так, если в 70-е годы объем суммарных знаний человечества увеличивался вдвое за 10 лет, в 80-е годы – за 5 лет, в 90-е годы — каждый год, то в начале XXI века – счет пошел на месяцы….** Подобное положение дел породило целый ряд новых определений высокоиндустриального общества, среди которых такие, как «Knowledge Society», «Knowledgeable Society» и т.п.

Резюмируя существующие подходы к трактовке понятия «глобальное информационное общество», можно сказать, что в настоящее время под таковым понимается:

---

[49] *Черешкин Д.С., Смолян Г.Л.* Сетевая информационная революция // Информационные ресурсы России.1997. № 4. С. 15–18.

[50] *Моисеев Н.* Информационное общество как этап новейшей истории // Свободная мысль. 1996. № 1. С. 81–83.

- общество нового типа, формирующееся в результате новой глобальной социальной революции, основой которой является взрывное развитие и конвергенция ИКТ;
- общество знания, в котором главным условием благополучия каждого человека и каждого государства становится знание, полученное благодаря беспрепятственному доступу к информации и умению с ней работать;
- глобальное общество, в котором обмен информацией не будет иметь ни временных, ни пространственных, ни политических границ; где с помощью научной обработки данных и поддержки знания будут приниматься более продуманные и обоснованные решения с целью улучшения качества жизни во всех ее аспектах;
- общество, которое, с одной стороны, способствует взаимопроникновению культур, а с другой, открывает каждому сообществу новые возможности для самореализации.

Таким образом, информационное общество возникает в рамках существующих индустриальных и постиндустриальных обществ с разной степенью интенсивности, но в соответствии с общими закономерностями, анализ которых позволяет выработать рекомендации, ускоряющие процесс его формирования в сбалансированных интересах личности, общества и государства.

1.2.2. Признаки и базовые черты информационного общества

Большинство экспертов выделяют следующие четыре внутренне связанные сущностные черты формирующегося информационного общества:

1. Изменение роли информации и знания в жизни общества, выразившееся, прежде всего, в беспрецедентном возрастании информационной насыщенности экономической, управленческой и других сфер деятельности, в превращении информации и знания в важнейший ресурс социально-экономического развития.

2. Превращение информационной индустрии в наиболее динамичную, выгодную и престижную сферу производства, которая обеспечивает лидирующую роль отдельных стран и регионов в системе мировой экономики.

3. Возникновение развитой рыночной инфраструктуры потребления информации и информационных услуг и, в частности, широкое внедрение ИКТ в различные сферы жизни, причем не только в профессиональную, но и бытовую.

4. Глубокие изменения в моделях социальной организации и сотрудничества, когда во всех сферах общества происходит замена централизованных иерархических структур гибкими сетевыми типами организации, приспособленными к быстрым изменениям и инновационному развитию.

При этом происходящие изменения, как правило, обуславливают следующие факторы:

- Окончательно оформившаяся в середине XX века тесная связь науки и технических разработок, повлекшая за собой резкий рост динамики производства и появление наукоемких технологий.
- Глобализация всех происходящих в обществе изменений, когда события, территориально очень далекие друг от друга, оказываются звеньями одной цепи, утрачивая тем самым свой, казалось бы, локальный характер.
- Колоссальное усложнение всей экономической, политической, военной деятельности человечества и формирование здесь сложных систем, что выдвинуло на первый план проблемы управления и его информационного обеспечения, породив не только такие области знания, как кибернетика, системный анализ, исследование операций, но и новое мировоззрение, в рамках которого мир воспринимается через призму информационных процессов.
- Развитие новых ИКТ, широкое внедрение которых во все сферы жизни человека привело к их серьезной перестройке и появлению таких новых форм социальной и экономической деятельности, как электронная коммерция, телеработа, дистанционное образование, телемедицина и электронная демократия.

До сих пор, несмотря на широкое распространение термина информационное общество, эксперты еще не пришли к единому пониманию его основного содержания. Существует целый ряд определений, которые выдвигают на передний план те или иные его реальные черты и тенденции.

Так, например, очевидна тенденция увеличения доли занятых обработкой информации в структуре занятости в развитых странах. По расчетам С.Барли, к началу XXI века доля американцев, чей труд в основном связан с физическим трудом в сфере производства или услуг (сельхозрабочие, ремесленники, механики, работники гостиниц, розничные торговцы, парикмахеры и т.п.), должна сократиться вдвое (с 83% в начале XX века.). Одновременно должна увеличиться доля тех, кто работает в основном с информацией, с 17% до 59%. **В силу**

этого одно из самых распространенных определений информационного общества — это общество, в котором обработкой информации занято больше людей, чем обработкой сырья и материалов.

С точки зрения американского экономиста Т.Стюарта информационный век наступил в 1991 г., когда американские компании впервые затратили на приобретение компьютерной техники больше, чем на оборудование, предназначенное для работы с материальными ресурсами (двигатели, турбины, станки и механизмы, машины и т.п.).

В центре внимания многих работ находятся быстрое развитие ИКТ и их возрастающее использование во всех сферах экономической и общественной жизни. ИКТ существенно изменили за последние годы то, как мы учимся, работаем, занимаемся общественной деятельностью и отдыхаем. Более того, цифровые технологии активно проникают в традиционные технологии, меняя их возможности и сферы использования. Все это позволяет говорить о компьютерной, телекоммуникационной или микроэлектронной революции (Д.Е.Сайчел, Т.Форестер) и считать информационное общество обществом информационных технологий.

Перестройка мировой экономики, начавшаяся в середине 1970-х годов, привела к смене доминирующей формы организационной структуры предприятия и межфирменного сотрудничества. Целью организационных изменений была адаптация к резко возросшим темпам изменений в экономической, институциональной и технологической среде деятельности фирм. Общее направление изменений — переход от вертикальных иерархических структур к гибким сетевым формам организации, причем сети стали формообразующей основой внутренней организации современной корпорации, так и ее взаимодействия с партнерами (межфирменные сети, корпоративные стратегические альянсы и т.п.). Аналогичные организационные изменения происходят в сфере услуг, административных органах и других областях деятельности. Развитие ИКТ стимулировало происходящие изменения, позволило выявить все преимущества новой формы социальной организации, хотя организационные изменения возникли и развивались первоначально независимо от технологического развития. Со своей стороны, развитие телекоммуникационной инфраструктуры, и прежде всего Интернета, привело к тому, что все больше транзакций в современной экономике и обществе совершается с использованием компьютерных сетей. Интернет становится глобальной средой общения, труда и отдыха. Стремительно растут доходы от электронной коммерции, которые по прогнозам к 2007 г. увеличатся до нескольких триллионов USD. Указанные тенденции позволяют

многим специалистам говорить об информационном обществе как о «сетевом обществе», а современную экономику определять как «сетевую».

В последнее десятилетие с информационным обществом связываются большие ожидания. Считается, что оно обладает гигантским потенциалом для улучшения качества жизни всего человеческого сообщества и каждого человека в отдельности, резко расширяет возможности для малого и среднего предпринимательства, для оптимального использования местных условий и ресурсов, для развития сложных услуг и образования. Развитие информационного общества формирует предпосылки для значительного повышения эффективности производства, для экономии природных ресурсов и защиты окружающей среды, для перехода к устойчивому развитию.

Возникновение глобальных информационных сетей и систем впервые в истории нашей планеты открывает возможность связать буквально каждого с каждым, обеспечить доступ к информационным ресурсам человеческой цивилизации любому жителю Земли, объединить сегодняшние знания и духовные ценности, а, значит существенно раздвинуть границы применения достижений культуры, науки и техники.

Сегодня четко обозначилась тесная связь между образованием, обучением и развитием, поэтому ключевым фактором для любой отрасли, организации или компании становится эффективный доступ к образованию и непрерывное обучение. Во многих странах реальностью становится развертывание массовой системы качественного обучения на расстоянии, не ограниченного возрастными рамками.

Еще одна возможность, предоставляемая информационным обществом, — качественное улучшение системы охраны здоровья. Новые ИКТ делают широко доступной профилактическую информацию, создают основу для получения любым пациентом, где бы он ни жил, регулярных врачебных консультаций. Они превращают в реальность «телемедицину», опирающуюся на национальные и мировые информационные ресурсы в этой сфере.

В информационном обществе обычным явлением становится «телеработа», которая в состоянии кардинально решить проблему занятости, в том числе для людей с ограниченными физическими возможностями, что может помочь решению одной из самых сложных социальных проблем. Кроме того, с массовым распространением телеработы связываются надежды на решение такой острой проблемы больших городов как перегрузка транспортной системы и загрязнение воздуха выхлопными газами.

1.2.3. Социальные аспекты информационного общества

Информация становится реальным социальным ресурсом — ибо фактически только она способна помочь человеку адаптироваться к жизни в условиях постоянных изменений, выработать новые стереотипы поведения, соответствующие новым обстоятельствам. Для человека информационного века единство мира оказывается уже не теоретической или идеологической абстракцией, а фактом его повседневной жизни. «Сжимая пространство», информационное общество резко расширяет возможности человека выбирать, где и на каких условиях работать, у кого и по каким ценам покупать те или иные товары и услуги, делает продавцов более зависимыми от потребителей, существенно усложняют жизнь монополистам, недобросовестным работодателям и производителям.

Использование спутников, «живого» радио и телевидения для передачи информации оказывает массированное влияние на формирование общественного мнения по всему миру. Появление и бурное развитие мультимедиа, видеоконференций и интеллектуальных технологий кардинально расширяют возможности передачи информации, распространения знаний и обмена ими.

Важнейшей особенностью информационного общества является перенос акцента в производстве с использования материалов на производство информации и оказание услуг, что влечет за собой значительное снижение добычи и переработки сырья и расхода энергии.

Осознавая все преимущества информационного общества, нельзя, однако, не признать, что оно несет с собой не только новые решения и возможности, но и новые проблемы и риски.

ГИО приводит к размыванию национальных и политических границ и к ускорению темпов индустриализации и унификации культур — частично за счет образования глобальных конгломератов в области информации, телекоммуникаций и досуга.

Главная опасность заключается в том, что усиливающаяся глобализация производства и мобильность всемирных корпораций может неблагоприятным образом повлиять на экологическую политику, а также на труд и социальную защиту — причем во всемирном масштабе. Реальным сигналом тревоги является сокращение рабочих мест в компаниях, связанных с производством ИКТ, в наиболее развитых странах.

Все большее распространение «экранной» культуры, неизбежность столкновения с виртуальной реальностью, в которой трудно различимы иллюзия и действительность, создают некоторые проблемы психологического характера. По мере нарастания объема информации

людям становится труднее ориентироваться в ее содержании, ограждать себя от ее избытка.

В условиях существования открытых, легко доступных и легко наполняемых информационных сетей возникает проблема ограничения информации, считающейся социально и экономически опасной, проблема безопасности персональных и других видов данных, проблема соблюдения авторских прав и прав производителей электронной информации.

Развитие и широкое использование ИКТ привело к появлению еще одного измерения бедности, — так называемой «**информационной бедности**». Это понятие отражает рост социальной дифференциации населения по новому принципу — принципу возможностей доступа к современным ИКТ, когда лишь часть населения получает доступ к новейшим технологиям и информационным ресурсам и может реализовать это преимущество.

Благодаря ускорению процесса технологической инновации, вовлечению индустриального капитала и конкуренции новая сетевая технология и инфраструктура становятся гораздо дешевле, а потому доступнее для все большего числа людей. Что же касается доступа к распространяемой по ним информации, то это остается одной из самых сложных проблем. Стоимость информационных услуг может на многие годы стать фактором, усиливающим разрыв между теми, кто может и кто не может получать и распространять информацию.

Эксперты справедливо ставят следующие вопросы, на которые до сих пор не получены исчерпывающие ответы:

- Какова роль владельцев инфраструктуры, производителей программных продуктов, авторов, издателей, правительств и международных организаций в широком распространении информации в тех слоях населения или в тех странах, где доступ к информационным ресурсам недостаточен?
- Как добиться баланса между дешевой или бесплатной информацией, распространяемой для широкого круга пользователей правительствами и международными организациями, и интеллектуально насыщенными информационными продуктами, обеспечивающими эффективный доступ к знанию и принятие эффективных решений?

Решение этих и других проблем становления информационного общества требует серьезных усилий специалистов самых разных профилей. При этом необходимо принимать в расчет, что методы противодействия всем перечисленным и другим опасностям инфор-

мационного века лежат не в области отгораживания себя от ГИО, а в сфере развития собственного полноценного участия в его формировании.

Как и любое другое, информационное общество несовершенно, а ИКТ нейтральны — последствия их применения целиком зависят от ценностных установок и политических решений. В силу этого реализация возможностей информационного общества — вопрос адекватной политики и своевременных управленческих решений.

Информационное общество отличается от общества, в котором доминируют традиционная промышленность и сфера услуг, тем, что информация, знания, информационные услуги и все отрасли, связанные с их производством (телекоммуникационная, компьютерная, телевизионная), растут более быстрыми темпами, являются источником новых рабочих мест, становятся доминирующими в экономическом развитии. Для того, чтобы оценить этот процесс количественно, необходимо иметь соответствующие статистические данные. Однако здесь имеются трудности, поскольку статистическая система инерционна, вводит новые показатели измерений с серьезным запаздыванием.

Развитие ИКТ породило не только разнообразные социальные эффекты, но и привело к возникновению нового течения общественной мысли, известного под названием теории информационного общества. Ведущие исследователи сходятся во мнении, что данная теория находится в самом начале своего становления, хотя первые работы по этой тематике появились в 60—70-х годах и носили не столько научный, сколько футуристический характер, иногда смыкаясь с научно-фантастической литературой.

Несмотря на достаточную распространенность самого термина «информационное общество», разработанной концепции его еще не предложено. Нередко в литературе можно встретить лишь оптимистичные прогнозы и ожидания, хотя очевидно, что переход к массовому использованию новейших ИКТ неизбежно породит серьезный социальный стресс, даст техническую возможность группам людей, владеющим СМИ, контролировать все общество и каждого человека. Именно с целью предотвращения этих негативных последствий перехода к информационному обществу необходима четко выверенная под конкретные условия государственная политика.

Сегодня технологическая составляющая общественного развития существенно более значима, чем она была в начале века, а скорость происходящих под ее воздействием изменений столь вели-

ка, что на глазах одного поколения происходит несколько циклов технологического обновления. Соответственно появляются и возможности для общих выводов, в том числе и философского характера.

Взаимосвязь «общество — новейшие технологии» всегда была традиционным объектом философских исследований. Специфика современной ситуации состоит в том, что изменения в информационной индустрии столь стремительны и обладают столь всеобщим действием, что приходится одновременно изучать процессы, как на эмпирическом, так и теоретическом уровнях и на их основе делать обобщения и строить рекомендации. Многие перспективные направления сегодня только намечаются, но они настолько быстро могут воплотиться в жизнь, что времени для выжидания, пока они окончательно оформятся, просто нет.

В силу этого столь необходимы анализ становления информационного общества, выработка стратегии, позволяющие государству вместе с частным сектором, промышленностью и научно-технической интеллигенцией определить цели и задачи на пути к ГИО.

На каждой новой ступени технологического развития общества появляется работа для обществоведов, философов, задача которых не только оценить последствия происходящих процессов, но и дать прогнозы развития, выработать методологические рекомендации политикам. К сожалению, приходится констатировать, что современный российский политический истеблишмент пока еще не полностью проникся важностью проблематики ГИО. Посткризисное развитие экономики, обострение ряда социальных проблем заставляют решать, прежде всего, сиюминутные задачи. Проблема в России усугубляется благоприятным уровнем мировой конъюнктуры цен на энергоносители. Однако есть уверенность, что объективные тенденции становления информационного общества заставят политиков обратить на себя внимание, потребуют включить меры по его формированию в свои избирательные программы и политические платформы. И это время не за горами.

Резюмируя, можно подчеркнуть, что ГИО — это не умозрительная конструкция, некий идеальный образ будущего, который в очередной раз предлагают исследователи в качестве ориентира, а эволюционное развитие индустриального общества, в котором стремительными темпами растут секторы, связанные с созданием и потреблением информации.

Глава 2
МЕЖДУНАРОДНОЕ СООБЩЕСТВО И ГИО

2.1. Организация Объединенных Наций и ИКТ

Рубеж веков ознаменовался резкой активизацией деятельности международных организаций и различных структур по изучению и продвижению различных аспектов ГИО. Одной из первых данной проблематикой в силу ее глобальности занялась ООН. Даже беглый синопсис обсужденных проблем действительно впечатляет.

Начиная с 1976 г. по 2004 г. в ООН по проблематике ИКТ или маргинальным с ней вопросам приняты нижеследующие 19 резолюций Генеральной Ассамблеи, а также рассмотрены 15 докладов и записок Генерального секретаря ООН:

A/RES/59/61[1]	3 декабря 2004 года	Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности
A/RES/58/272	10 ноября 2003 года	Стратегия в области информационно-коммуникационных технологий
A/RES/58/199	23 декабря 2003 года	Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур (Содержит «**Элементы для защиты важнейших информационных инфраструктур**»)

[1] http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/RES/59/61&Lang=R (см. Приложение).

A/RES/58/32	8 декабря 2003 года	Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности
A/RES/57/304	15 апреля 2003 года	Стратегия в области информационно-коммуникационных технологий
A/RES/57/295	20 декабря 2002 года	Использование информационно-коммуникационных технологий в целях развития
A/RES/57/239	20 декабря 2002 года	Создание глобальной культуры кибербезопасности (Содержит «**Элементы для создания глобальной культуры кибербезопасности**»)
A/RES/57/53	22 ноября 2002 года	Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности
A/RES/56/281	1 мая 2002 года	Участие в пленарных заседаниях в рамках заседания Генеральной Ассамблеи, посвященного использованию информационно-коммуникационных технологий в целях развития
A/RES/56/258	31 января 2002 года	Заседание Генеральной Ассамблеи, посвященное использованию информационно-коммуникационных технологий в целях развития
A/RES/56/239	24 декабря 2001 года	Информационная технология
A/RES/56/121	19 декабря 2001 года	Борьба с преступным использованием информационных технологий
A/RES/56/19	29 ноября 2001 года	Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности
A/RES/55/63	4 декабря 2000 года	Борьба с преступным использованием информационных технологий
A/RES/55/28	20 ноября 2000 года	Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности
A/RES/54/49	1 декабря 1999 года	Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности
A/RES/53/70	4 декабря 1998 года	Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности
A/RES/32/178	19 декабря 1977 года	Сеть для обмена технической информации и банк промышленно-технической информации
A/RES/31/183	21 декабря 1976 года	Создание сети для обмена технической информации

Доклады и записки Генерального секретаря

A/59/265	3 сентября 2004 года	Стратегия в области ИКТ
A/58/740	18 марта 2004 года	Функциональные потребности полевых миссий в ИКТ
E/CN.3/2004/16	30 января 2004 года	Доклад Международного союза электросвязи о статистических данных по ИКТ
A/58/568	12 ноября 2003 года	Использование ИКТв целях развития: ход осуществления резолюции 57/295 Генеральной Ассамблеи
A/58/377	18 сентября 2003 года	Стратегия в области ИКТ: осуществление резолюции 57/304 Генеральной Ассамблеи от 15 апреля 2003 года
E/2003/56	28 апреля 2003 года	Первый ежегодный доклад Целевой группы по информационно-коммуникационным технологиям
E/CN.6/2003/6	30 декабря 2002 года	Участие женщин в работе средств массовой информации и освоении коммуникационных технологий и их доступ к ним, а также их влияние на улучшение положения и расширение возможностей женщин и их использование в качестве средства для достижения этих целей
A/57/620	20 ноября 2002 года	Стратегия в области ИКТ
E/2002/64	14 мая 2002 года	Осуществление согласованных выводов 2000/1 Экономического и Социального Совета о роли ООН в поощрении развития, в частности в том, что касается доступа к знаниям и технологиям и их передачи, особенно ИКТ, в частности в рамках отношений партнерства с соответствующими заинтересованными сторонами, включая частный сектор
E/2001/59	2 мая 2001 года	Роль ООН в поощрении развития, в частности в том, что касается доступа к знаниям и технологиям и их передачи, особенно ИКТ, в частности в рамках отношений партнерства с соответствующими заинтересованными сторонами, включая частный сектор
E/2001/7	20 февраля 2001 года	Целевая группа по ИКТ
A/55/780	13 февраля 2001 года	Информационная технология в Секретариате: План действий
A/55/75-E/2000/55	22 мая 2000 года	Доклад группы экспертов высокого уровня по ИКТ
E/2000/52	18 мая 2000 года	Развитие и сотрудничество в XXI веке: роль информационной технологии в контексте основанной на знаниях глобальной экономики
A/54/849	1 мая 2000 года	Информационные технологии

2.1.1.Целевая группа ЭКОСОС по ИКТ

Экономический и Социальный Совет (ЭКОСОС) ООН, исходя из декларации министров, поручил Генеральному секретарю ООН создать Целевую группу по ИКТ[2]. Эта инициатива была призвана перевести на поистине глобальный уровень всю совокупность мероприятий по преодолению цифрового разрыва, развить цифровые возможности и тем самым прочно поставить ИКТ на службу развитию для всех. Импульс созданию Целевой группы по ИКТ был дан состоявшимся в апреле 2000 г. под эгидой ООН заседанием группы независимых экспертов, представлявших различные сферы экономики, академические круги, гражданское общество и правительственные структуры.

Чтобы достичь ощутимых и устойчивых результатов в области ИКТ для развития, необходимо не только действовать на местном уровне, развивать сотрудничество на субрегиональном и региональном уровнях, но и вырабатывать на глобальном уровне общую повестку дня. Вклад ООН в это дело, осуществляемый через Целевую группу по ИКТ, реализует уникальные преимущества Организации, а именно ее легитимность, универсальность, глобальный размах ее деятельности в области развития, опыт работы на местах, равно как и ее способность служить катализатором и собирать вместе всех участников.

Задача Целевой группы состоит в том, чтобы обеспечить общее лидерство по отношению к роли ООН в деле содействия в формулировании стратегий развития ИКТ и постановки этих технологий на службу развитию. Кроме того, в задачу Группы входит формирование, на базе консультаций со всеми заинтересованными участниками и странами-членами, стратегического партнерства между системой ООН, частным бизнесом, финансовыми трестами и фондами, донорами, странами, в которых осуществляются программы помощи и прочими участниками, в соответствии с относящимися к этому вопросу резолюциями ООН.

Задачи Целевой группы получили дальнейшую поддержку в ходе Саммита тысячелетия[3] и в принятой им Декларации тысячелетия[4].

Целевая группа представляет собой механизм, созданный на основе решения межправительственного органа ООН, в котором все его члены, представляющие правительства, гражданское общество, а так-

[2] http://www.unicttaskforce.org/

[3] http://www.un.org./russian/conferen/millennium/summit.htm

[4] http://www.un.org/russian/documen/declarat/summitdecl.htm

же организации системы ООН, имеют равные права в плане принятия решений.

Целевая группа по ИКТ призвана содействовать реализации принятых на международном уровне комплексных целей и задач развития, в частности тех, которые содержатся в Декларации тысячелетия. Главной задачей и мерилом успеха всей деятельности Целевой группы является искоренение нищеты и обеспечение особых нужд Африки, наименее развитых стран и стран с низким доходом. Целевая группа нацелена на то, чтобы избежать дублирования работы других участников и послужить катализатором в деле укрепления синергетических связей и упрочения последовательности общих усилий. С этой целью Целевая группа тесно сотрудничала с созданной «восьмеркой» Целевой группой по возможностям использования цифровой технологии[5], равно как и с другими глобальными инициативами, в том числе инициативами Всемирного экономического форума[6], Глобального диалога бизнеса по вопросам электронной торговли[7], и др.

Целевая группа способна внести ощутимый вклад в таких жизненно важных областях, как содействие развитию образования, борьба с заболеваниями, упрочение равенства полов и развитие возможностей женщин, молодежи, инвалидов и вообще бедных. Соответствующие инициативы, выдвинутые Генеральным секретарем (включая ВИЧ/СПИД, Технологические добровольцы, Сеть здравоохранения[8], обучение девочек и занятость молодежи), получили поддержку со стороны Целевой группы. В этом плане Целевая группа опирается на деятельность ныне существующих организаций системы ООН, занимающихся развитием, и специализированных организаций ООН. Она также участвует в работе Всемирной встречи на высшем уровне по вопросу ГИО (2003 и 2005 гг.).

Для достижения этих целей Целевая группа завязывает сотрудничество с правительственными органами, предпринимательским сектором, неприбыльными организациями, академическим сообществом, международными организациями, гражданским обществом и неправительственными организациями, равно как и с другими подобными инициативами и мероприятиями на всех уровнях. Образ действия Целевой группы основан на децентрализации, открытости, вовлечении всех участников, а также на опоре, насколько это возможно, на

[5] http://www.dotforce.org/

[6] http://www.weforum.org/

[7] http://www.gbde.org/index.html

[8] http://www.healthinternetwork.net/

уже действующие механизмы и программы. Целевая группа стремится к опоре на действующие, формирующиеся и новые инициативы и фокусируется на внесение своего вклада в их деятельность путем содействия упрочению и развертыванию этих мероприятий, а также содействия и поддержки координации и сотрудничества между всеми участниками.

В деле разработки стратегий и политики Целевая группа получает помощь со стороны Группы Советников высокого уровня, в которую входят эксперты, обладающие опытом работы в области ИКТ для развития и в смежных областях.

Краткое изложение полномочий Целевой группы:

- служить механизмом содействия и пропаганды в отношении совместных инициатив с участием, при необходимости, государственного и частного секторов, фондов и трестов в целях мобилизации ресурсов для программ и проектов в области ИКТ и для содействия их разработке и финансирования;
- выявлять и мобилизовывать новые ресурсы, как в государственном, так и в частном секторе;
- содействовать эффективному использованию имеющихся ресурсов в области ИКТ в целях развития;
- содействовать совместным инициативам по просьбе стран осуществления программ и в консультации с ними в отношении программ и проектов в области ИКТ, в т.ч. на региональном, субрегиональном и национальном уровнях, принимая во внимание положения пунктов 14-17 декларации министров, принятой на этапе заседаний высокого уровня основной сессии ЭКОСОС 2000 г.;
- содействовать совместному использованию соответствующего опыта как развитых, так и развивающихся стран и извлеченных уроков в области внедрения и распространения ИКТ при подготовке материалов местными силами и их использовании для сохранения и распространения традиционных знаний в целях содействия программным инициативам Север—Юг и Юг—Юг, создавать сети связи с другими механизмами и учреждениями как в государственном, так и в частном секторе, которые занимаются разработкой ИКТ, в целях повышения согласованности и выявления совместных программных инициатив;
- управлять целевым фондом, созданным всеми заинтересованными сторонами на основе добровольных взносов;
- состав Целевой группы сбалансирован с точки зрения представленности участников (система ООН, государственный и частный секторы, фонды, тресты, развитые и развивающиеся страны, а также страны с переходной экономикой);

• работу Целевой группы обеспечивает секретариат, состоящий из откомандированных участниками сотрудников и финансируемый за счет накладных расходов по программам и проектам, финансируемым за счет средств целевого фонда;

• Генеральный секретарь ООН представляет в ЭКОСОС для рассмотрения ежегодный доклад о деятельности Целевой группы.

Первый доклад Целевой группы (E/2003/56 от 28 апреля 2003 г.) был представлен ЭКОСОС на его сессии 2003 г. Совет приветствовал успехи, достигнутые Целевой группой, ее ориентацию на использование ИКТ для достижения целей в области развития, поставленных в Декларации тысячелетия. Было констатировано, что Целевая группа стала общепризнанным глобальным форумом по ИКТ.

С учетом того, что наиболее полно о деятельности Целевой группы было доложено во время второго годового отчета (Нью-Йорк, 28 июня — 23 июля 2004 г.), а также третьего отчета (Нью-Йорк, 29 июня — 27 июля 2005 г.) представляется оправданным привести наиболее важные компоненты из данных докладов[9].

Доклады были подготовлены в контексте выполнения мандата, содержащегося в резолюции 2000/29 ЭКОСОС от 28 июля 2000 года о Целевой группе по ИКТ, в которой Совет одобрил рекомендации Специальной рабочей группы открытого состава по информатике, содержащиеся в приложении к этой резолюции. В своем решении 2001/210 от 13 марта 2001 г. Совет просил Генерального секретаря принять необходимые меры для учреждения Целевой группы, как это рекомендовано в его докладе (E/2001/7), в пункте 35 которого говорится, что Генеральный секретарь будет ежегодно представлять ЭКОСОС доклад о работе Целевой группы.

В докладах содержится краткий обзор условий, в которых работала Целевая группа, описываются ее основные мероприятия и достижения, а также излагается стратегия, которую Группа намерена проводить в жизнь до конца 2005 г. (приняв во внимание ту роль, которую Целевая группа играет в деятельности по итогам женевского этапа ВВУИО общества и подготовке к тунисскому этапу в ноябре 2005 г., Генеральный секретарь ООН продлил мандат Целевой группы до конца 2005 г.).

Второй раздел второго доклада называется «Что происходит с «цифровым разрывом?», который базируется на данных Международного союза электросвязи (МСЭ).

---

[9] http://daccessdds.un.org/doc/UNDOC/GEN/N04/342/47/PDF/N0434247.pdf?OpenElement

2.1.2. Глобальный индекс стран мира доступа к цифровым технологиям (ДЦТ)

Чтобы оценить неравенство в плане доступа населения различных стран мира к ИКТ, МСЭ обобщил и проанализировал различия между развитыми и развивающимися странами[10] с точки зрения распространенности различных ИКТ (телефон, мобильный телефон, Интернет и компьютеры) в последнее десятилетие. Этот разрыв заметно сократился, причем особенно быстро он сокращался в таких областях, как мобильная связь и доступ к сети Интернет.

Средний уровень их распространенности в развивающихся странах в 2002 г. (4,1 пользователя Интернета и 10,7 абонента мобильных телефонов на 100 человек населения) соответствовал уровню, достигнутому в развитых странах около пяти лет назад. Средний же уровень стационарных телефонных линий в развивающихся странах (менее одной на 10 человек населения) был достигнут в развитых странах в 60-е годы.

Публикация первого глобального индекса ДЦТ принесла сюрпризы. Словения оказалась на одном уровне с Францией, а Республика Корея, которая, не входила в первую десятку по международным показателям доступа к ИКТ, вышла на четвертое место. Помимо Канады, которая находится на десятом месте, в первую десятку стран входят только страны Азии и Европы.

Индекс ДЦТ отличается от других индикаторов тем, что в него включен ряд новых показателей, таких, как образование и доступность. Кроме того, этот индекс классифицирует в общей сложности 178 стран, что делает его первым действительно глобальным показателем доступа к ИКТ.

Страны разделены на четыре категории по доступу к цифровым технологиям: самый широкий, широкий, средний и низкий. В категорию широкого доступа вошли главным образом страны Центральной и Восточной Европы, Карибского бассейна, государства Залива и быстро развивающиеся страны Латинской Америки. Многие из них использовали ИКТ в качестве катализатора развития. В качестве примера можно привести крупнейшие проекты в области ИКТ, такие, как Интернет-город в Дубае в ОАЭ, мультимедийный

[10] В категорию «развитые страны» отнесены Западная Европа, Австралия, Канада, Япония, Новая Зеландия и Соединенные Штаты. В категорию «развивающиеся страны» — остальные страны.

суперкоридор в Малайзии (которая заняла самое высокое место среди развивающихся стран Азии) и кибер-город в Маврикии (который наряду с Сейшельскими островами занял самое высокое место среди африканских стран). ДЦТ станет полезным критерием оценки дальнейшего развития этих быстро развивающихся стран.

Четыре «азиатских тигра» добились наибольшего прогресса в сфере ИКТ за последние четыре года. Это свидетельствует о том, что английский язык перестал быть решающим фактором в деле оперативного внедрения технологий, особенно благодаря тому, что стали появляться новые материалы на других языках.

Данные нового индекса ДЦТ свидетельствуют о том, что настало время пересмотреть потенциал доступа к ИКТ. «До настоящего времени недостаточный уровень развития инфраструктуры часто считался основным препятствием в преодолении отставания в сфере цифровых технологий, — говорит Майкл Мингс, представитель Группы по рынкам, экономике и финансам МСЭ, — вместе с тем проведенные нами исследования свидетельствуют о том, что доступность и уровень образования являются столь же важными факторами». Для оценки общего потенциала отдельных лиц в плане доступа к ИКТ и их использованию в рамках проведенного МСЭ исследования помимо традиционных вопросов инфраструктуры телекоммуникаций, которыми, прежде всего занимается эта организация, были освещены такие аспекты, как мобильные телефоны и обычные телефонные линии.

Например, почти 40 процентов перуанцев, принявших участие в опросе, указали, что у них нет компьютера или нет доступа к Интернету. Исследования также показали, что использование Интернета тесно связано с образованием. В Китае свыше половины всех пользователей Интернета имеют университетское образование. Для учета этого фактора в индекс включен ряд новых критериев, таких, как размер платы за обучение и за доступ к Интернету в качестве доли от дохода.

В ДЦТ включено 8 показателей, охватывающих 5 областей, которые определяют общее положение страны. Эти области включают наличие инфраструктуры, приемлемый уровень расходов для получения доступа, уровень образования, качество услуг в области ИКТ и использование Интернета. Этот индекс определяет потенциальные препятствия в сфере применения ИКТ и может явиться для стран подспорьем в определении их относительно сильных и слабых сторон.

ДЦТ позволяет преодолеть ограничения, присущие другим индексам в области ИКТ. Отобранные критерии обеспечивают не только его глобальный характер, но и прозрачность. Из него преднамеренно исключены показатели, допускающие качественную оценку.

Усилия МСЭ по разработке показателей для оценки доступа к ИКТ являются свидетельством ширящейся в международном сообществе тенденции к применению прозрачных и конкретных критериев оценки положения в странах. ООН разработала ряд целевых показателей в сфере развития — цели в области развития, сформулированные в Декларации тысячелетия, и соответствующие индикаторы оценки прогресса в деле сокращения нищеты, голода и в других сферах. Доступ к ИКТ включен в цели в области развития, намеченные в Декларации тысячелетия, и сформулирован в задаче 18: «В сотрудничестве с частным сектором принимать меры к тому, чтобы все могли пользоваться благами новых технологий, особенно ИКТ». ДЦТ является конкретным средством для оценки прогресса в решении этой ключевой задачи.

Обсуждение вопросов ИКТ имеет особенно важное значение в связи с тем, что, как было признано, широкий доступ может способствовать экономическому развитию и улучшению жизни граждан. Интернет обеспечивает мгновенный доступ к информации из любой точки мира в любое время и является весьма перспективным средством в сфере улучшения здравоохранения, просвещения и охраны окружающей среды.

В полном тексте доклада приводится обзор показателей, применяемых для оценки ДЦТ (за 2002 г.); анализ применения ИКТ в предпринимательских кругах, в сфере просвещения и в государственных органах, а также оценка их роли в деле достижения целей в области развития.

Индекс доступа к цифровым технологиям

Самый широкий доступ		*Широкий доступ*		*Средний доступ*		*Низкий доступ*	
Швеция	0,85	Ирландия	0,69	Беларусь	0,49	Зимбабве	0,29
Дания	0,83	Кипр	0,68	Ливан	0,48	Гондурас	0,29
Исландия	0,82	Эстония	0,67	Таиланд	0,48	Сирия	0,28
Республика Корея	0,82	Испания	0,67	Румыния	0,48	Папуа-Новая Гвинея	0,26
Норвегия	0,79	Мальта	0,67	Турция	0,48	Вануату	0,24
Нидерланды	0,79	Чешская Республика	0,66	Бывшая югославская республика Македония	0,48	Пакистан	0,24

Гонконг, Китай	0,79	Греция	0,66	Панама	0,47	Азербайджан	0,24
Финляндия	0,79	Португалия	0,65	Венесуэла	0,47	Сан-Томе и Принсипи	0,23
Тайвань, Китай	0,79	ОАЭ	0,64	Белиз	0,47	Таджикистан	0,21
Канада	0,78	Макао, Китай	0,64	Сент-Винсент	0,46	Экваториальная Гвинея	0,20
Соединенные Штаты	0,78	Венгрия	0,63	Босния	0,46	Кения	0,19
Соединенное Королевство	0,77	Багамские Острова	0,62	Суринам	0,46	Никарагуа	0,19
Швейцария	0,76	Бахрейн	0,60	Южная Африка	0,45	Лесото	0,19
Сингапур	0,75	Сент-Китс и Невис	0,60	Колумбия	0,45	Непал	0,19
Япония	0,75	Польша	0,59	Иордания	0,45	Бангладеш	0,18
Люксембург	0,75	Словацкая Республика	0,59	Сербия и Черногория	0,45	Йемен	0,18
Австрия	0,75	Хорватия	0,59	Саудовская Аравия	0,44	Того	0,18
Германия	0,74	Чили	0,58	Перу	0,44	Соломоновы Острова	0,17
Австралия	0,74	Антигуа и Барбуда	0,57	Китай	0,43	Камбоджа	0,17
Бельгия	0,74	Барбадос	0,57	Фиджи	0,43	Уганда	0,17
Новая Зеландия	0,72	Малайзия	0,57	Ботсвана	0,43	Замбия	0,17
Италия	0,72	Литва	0,56	Иран (Исламская Республика)	0,43	Мьянма	0,17
Франция	0,72	Катар	0,55	Украина	0,43	Конго	0,17
Словения	0,72	Бруней-Даруссалам	0,55	Гайана	0,43	Камерун	0,16
Израиль	0,70	Латвия	0,54	Филиппины	0,43	Гана	0,16
		Уругвай	0,54	Оман	0,43	Лаосская Народно-Демократическая Республика	0,15
		Сейшельские Острова	0,54	Мальдивские Острова	0,43	Малави	0,15
		Доминика	0,54	Ливия	0,42	Танзания	0,15
		Аргентина	0,53	Доминиканская Республика	0,42	Гаити	0,15
		Тринидад и Тобаго	0,53	Тунис	0,41	Нигерия	0,15
		Болгария	0,53	Эквадор	0,41	Джибути	0,15
		Ямайка	0,53	Казахстан	0,41	Руанда	0,15
		Коста-Рика	0,52	Египет	0,40	Мадагаскар	0,15
		Сент-Люсия	0,52	Кабо-Верде	0,39	Мавритания	0,14
		Кувейт	0,51	Албания	0,39	Сенегал	0,14
		Гренада	0,51	Парагвай	0,39	Гамбия	0,13
		Маврикий	0,50	Намибия	0,39	Бутан	0,13
		Россия	0,50	Гватемала	0,38	Судан	0,13

		Мексика	0,50	Сальвадор	0,38	Коморские Острова	0,13
		Бразилия	0,50	Палестина	0,38	Кот-д'Ивуар	0,13
				Шри-Ланка	0,38	Эритрея	0,13
				Боливия	0,38	Демократическая Республика Конго	0,12
				Куба	0,38	Бенин	0,12
				Самоа	0,37	Мозамбик	0,12
				Алжир	0,37	Ангола	0,11
				Туркменистан	0,37	Бурунди	0,10
				Грузия	0,37	Гвинея	0,10
				Свазиленд	0,37	Сьерра-Леоне	0,10
				Молдова	0,37	Центрально-африканская Республика	0,10
				Монголия	0,35	Эфиопия	0,10
				Индонезия	0,34	Гвинея-Бисау	0,10
				Габон	0,34	Чад	0,10
				Марокко	0,33	Мали	0,09
				Индия	0,32	Буркина-Фасо	0,08
				Кыргызстан	0,32	Нигер	0,04
				Узбекистан	0,31		
				Вьетнам	0,31		
				Армения	0,30		

Примечания : По шкале от 0 до 1, где 1 составляет самый широкий доступ. Значения ДЦТ приведены с точностью до одной сотой. Страны с аналогичным ДЦТ ранжированы с учетом тысячных.

Важнейшие элементы индекса доступа к ДЦТ

Первые пять стран Африки к югу от Сахары				**Первые пять стран Арабского региона**			
Место	*Общий показатель*	*Страна*	*ДЦТ*	*Место*	*Общий показатель*	*Страна*	*ДЦТ*
1	52	Сейшельские Острова	0,54	1	34	Объединенные Арабские Эмираты	0,64
2	62	Маврикий	0,50	2	42	Бахрейн	0,584
3	78	Южная Африка	0,45	3	48	Катар	0,55
4	86	Ботсвана	0,43	4	60	Кувейт	0,51
5	99	Кабо-Верде	0,39	5	67	Ливан	0,53

Первые десять стран Американского континента							
Место	*Общий показатель*	*Страна*	*ДЦТ*	*Место*	*Общий показатель*	*Страна*	*ДЦТ*
1	10	Канада	0,78	6	44	Антигуа и Барбуда	0,57
2	11	Соединенные Штаты	0,78	7	45	Барбадос	0,57
3	37	Багамские Острова	0,62	8	51	Уругвай	0,54
4	38	Сент-Китс и Невис	0,60	9	53	Доминика	0,54
5	43	Чили	0,58	10	54	Аргентина	0,53

Первые пять развитых стран Азии и Тихого океана				Первые пять развивающихся стран Азии и Тихого океана			
Место	*Общий показатель*	*Страна*	*ДЦТ*	*Место*	*Общий показатель*	*Страна*	*ДЦТ*
1	4	Республика Корея	0,82	1	46	Малайзия	0,57
2	7	Гонконг, Китай	0,79	2	49	Бруней-Даруссалам	0,55
3	9	Тайвань, Китай	0,79	3	68	Таиланд	0,48
4	14	Сингапур	0,75	4	84	Китай	0,43
5	15	Япония	0,75	5	85	Фиджи	0,43

Первые пять стран Западной Европы				Первые пять стран Центральной и Восточной Европы			
Место	*Общий показатель*	*Страна*	*ДЦТ*	*Место*	*Общий показатель*	*Страна*	*ДЦТ*
1	1	Швеция	0,85	1	24	Словения	0,72
2	2	Дания	0,83	2	26	Эстония	0,69
3	3	Исландия	0,82	3	32	Чешская Республика	0,66
4	5	Норвегия	0,79	4	36	Венгрия	0,63
5	6	Нидерланды	0,79	5	39	Польша	0,59

Пять наиболее быстро развивающихся стран, 1998–2002 годы				Пять стран с наиболее резким снижением показателя, 1998–2002 годы			
Место 1998 год	*Место 2002 год*	*Страна*	*Изменение*	*Место 1998 год*	*Место 2002 год*	*Страна*	*Изменение*
24	4	Республика Корея	20	12	21	Новая Зеландия	-9
22	9	Тайвань, Китай	13	11	19	Австралия	-8
20	14	Сингапур	6	30	36	Южная Африка	-6
13	7	Гонконг, Китай	6	17	23	Франция	-6
7	2	Дания	5	5	11	Соединенные Штаты	-6
По 40 странам, в отношении которых имелись данные за 1998 год							

Техническое примечание к индексу ДЦТ

ДЦТ отражает общие возможности отдельных лиц в той или иной стране в плане доступа к ИКТ и их использования. Он состоит из 8 показателей, сгруппированных в 5 категорий. Каждый показатель приводится к индикатору со значением от 0 до 1, которой определяется путем его деления на максимальное значение или «целевой показатель». После этого каждый индикатор взвешивается в своей категории, а итоговые значения индекса усредняются для получения общего значения ДЦТ.

Категория	*Показатель*	*Значения для Гонконга, Китай*	*Целевой показатель*	*Показатель*	*Значение*	*Индекс категории*
1. Инфраструктура	1. Количество подписчиков обычных телефонных линий на 100 жителей	56,6 /	60 =	0,94 *	(1/2) =	0,47 + = 0,93
	2. Количество подписчиков мобильных сотовых телефонов на 100 жителей	91,6 /	100 =	0,92 *	(1/2) =	0,46
2. Доступность	3.1 — (Стоимость доступа к Интернету в качестве доли от ВНП на душу населения)	99,8 /	100 =	0,998 *	1 =	0,998
3. Уровень знаний	4. Уровень грамотности среди взрослых	93,5 /	100 =	0,94 *	(2/3) =	0,62 + = 0,83
	5. Общий показатель приема в начальную, среднюю и высшую школу	63,05 /	100 =	0,63 *	(1/3) =	0,21
4. Качество	6. Пропускная способность каналов доступа к международному Интернету (в битах) на душу населения	1'867 /	10'000 =	0,88a *	(1/2) =	0,44 + = 0,68
	7. Пропускная способность каналов на 100 жителей	14,6 /	30 =	0,49 *	(1/2) =	0,24
5. Использование	8. Количество пользователей Интернета на 100 жителей	43,0 /	85 =	0,51 *	1 =	0,51
Индекс ДЦТ (средний показатель по пяти приведенным выше категориям)						**0,79**

Примечание: В связи с разбросом значений показателей между странами для расчета этого значения использовался следующий логарифм: (LOG (1'867) – LOG (0.1)) / (LOG (10'000) – (LOG (O.01))

Первые пять стран по категориям ДЦТ, 2002 год

*Инфраструктура: первые пять стран по количеству подписчиков **обычных** телефонных линий на 100 жителей*

1	Швеция	65,25
2	Соединенные Штаты	65,02
3	Кипр	62,44
4	Канада	61,30
5	Тайвань, Китай	57,45

*Инфраструктура: первые пять стран по количеству подписчиков **мобильных** сотовых телефонов на 100 жителей*

1	Тайвань, Китай	106,5
2	Люксембург	105,4
3	Израиль	95,5
4	Италия	92,5
5	Гонконг, Китай	91,6

Доступность: первые пять стран по показателю оплаты за пользование Интернетом в качестве процентной доли дохода на душу населения

1	Гонконг, Китай	0,19
2	Соединенные Штаты	0,51
3	Сингапур	0,64
4	Дания	0,68
5	Канада	0,68

Примечание: Рассчитано на базе наиболее низкой ставки за 20 часов пользования Интернетом в месяц, поделенной на показатель дохода на душу населения, полученный от Всемирного банка.

Источник: МСЭ.

Уровень знаний: страны с самым высоким значением индекса образования ПРООН

	Уровень грамотности	*Прием в школы*	*Индекс образования*
Австралия	99	114	0,99
Бельгия	99	107	0,99
Дания	99	98	0,99
Финляндия	99	103	0,99
Нидерланды	99	99	0,99
Новая Зеландия	99	99	0,99
Норвегия	99	98	0,99
Швеция	99	113	0,99
Соединенное Королевство	99	112	0,99

Примечание: Индекс образования рассчитывается как (2/3) помноженные на показатель грамотности и (1/3) показателя приема в школы. Страны приводятся в алфавитном порядке. Методология и данные получены от ПРООН.

Качество: первые пять стран по количеству подписчиков услуг Интернета на 100 жителей

1	Республика Корея	21,9
2	Гонконг, Китай	14,6
3	Канада	11,1
4	Тайвань, Китай	9,4
5	Бельгия	8,4

Источник: База данных показателей ДЦТ МСЭ.

Качество: первые пять стран по пропускной способности каналов международного Интернета (в битах) на одного жителя

1	Дания	20'284
2	Швеция	10'611
3	Нидерланды	10'327
4	Швейцария	8'991
5	Бельгия	8'121

Источник: База данных показателей ДЦТ МСЭ.

Использование: первые пять стран по количеству пользователей Интернета на 100 жителей

1	Исландия	64,9
2	Швеция	57,3
3	Республика Корея	55,2
4	Соединенные Штаты	55,1
5	Япония	54,5

Источник: База данных показателей доступа к глобальным телекоммуникациям МСЭ.

В докладах Целевой группы по ИКТ делается вывод, что развивающиеся страны быстрее «догоняют» развитые в ИКТ, чем в иных отраслях. При этом было подчеркнуто то обстоятельство, что развивающиеся страны предпочитают мобильные телефоны стационарным, может затормозить развитие Интернета в ближайшем будущем, т.к. большинство пользователей Интернета в мире до сих пор соединяются с сетью по обычным телефонным линиям. Доступ в Интернет при помощи беспроводных устройств, разумеется, возможен (например, при помощи так называемых мобильных телефонов «третьего поколения» или беспроводных ЛВС), но он попрежнему достаточно дорог и имеет пока ограниченный радиус действия.

Эти проблемы разрешимы, но развитие Интернета в ряде регионов мира тормозится именно из-за недоразвитости обычной телефонной сети.

Выравнивание показателей распространенности ИКТ по всему миру произошло за последние несколько лет. В 2002 г. впервые число мобильных телефонов в мире превысило число стационарных. Африка стала первым регионом, где это произошло, и наиболее заметные последствия это имело для стран Африки к югу от Сахары. В Уганде и Демократической Республике Конго количество мобильных телефонов превышает количество стационарных почти в десять раз. В развитии телекоммуникации в Африке преодолен психологически важный порог одного пользователя на 100 человек населения. За первые несколько лет нового столетия к телекоммуникационным услугам приобщилось больше африканцев, чем за 100 лет предыдущей истории.

Однако существует опасность того, что при этом окажутся забытыми другие части мира и, в особенности, в малых островных государствах Тихоокеанского региона, которых пока не коснулись блага ИКТ. По показателю общей телефонной плотности Тихоокеанский регион был оттеснен с пятого на седьмое место. «Те, кто заявляет, что ИКТ дают развивающимся странам возможность «перепрыгнуть» целые этапы технического развития и тем самым начать конкурировать на основе знаний в области ИКТ с промышленно развитыми странами в более равных условиях, могут быть в определенной степени разочарованы. К моменту, когда большинство развивающихся стран внедрит «беспроводные сети второго поколения», значительное число развитых стран уже внедрит «сети третьего поколения», выполняющие более широкие функции. С другой стороны, закон Мура (см. параграф 1 главы 1) означает, что

и догонять можно значительно более быстрыми темпами. Например, если развитым странам потребовалось от 20 до 30 лет с тем, чтобы увеличить с 10 до 30 число телефонов (стационарных или мобильных) на каждые 100 жителей, многие развивающиеся страны сейчас показывают, что этого можно добиться менее чем за 10 лет.

Вместе с тем, существует множество примеров того, как ИКТ могут способствовать развитию через «самые передовые технологии», а также через то, что иногда называется «соответствующими технологиями». Удачным примером является проект wi-fi (беспроводного подключения к Интернету) в Дал-Лейке в Индии. С отменой лицензирования использования радиоспектра для широкополосной высокоскоростной пакетной передачи данных широкополосная связь была расширена (с использованием технологии wi-fi) на малонаселенные районы. Этот проект является революционным и может широко копироваться.

Данный пример показывает, что переносной Интернет может стать так называемой «прорывной технологией». Эта технология действительно может помочь «проскочить» традиционные (весьма длительные) циклы сетевых систем и избежать высоких расходов на них. Понятие «переносной Интернет» является общим термином, который используется для описания платформы высокоскоростного доступа к данным с использованием Интернет-протокола, и охватывает передовые беспроводные технологии, такие, как wi-fi, WiMAX, IMT-2000 direct spread, 3G, датчики ультраширокополосной и радиочастотной идентификации, работающие на большие, средние и короткие расстояния, и новые методы, которые позволяют более эффективно использовать имеющийся спектр, включая широкополосный, «умные антенны», быстронастраиваемые радиоприемники и сотовые сети.

По сути, цивилизация столкнулась с двойной задачей: обеспечить подключение населения Земли к Интернету и использовать это подключение для содействия устойчивому развитию.

Одним из основных вопросов повестки дня развития является вопрос об имеющихся у развивающихся стран вариантах финансирования их попыток содействия росту использования ИКТ. Финансирование инфраструктуры ИКТ в развивающихся странах традиционно обеспечивалось либо из госбюджета, либо из доходов почтово-телеграфных служб, или же донорами через международные финансовые учреждения.

2.2. Партнерство ООН с другими международными организациями и структурами

Основу мандата Целевой группы по ИКТ составляют партнерские связи и тот синергетический эффект, который они создают. Целевая группа опирается на результаты работы, ведущейся другими группами по возможностям использования цифровой технологии «восьмерки» и других сетей, таких, как Интернет-сеть по вопросам здравоохранения, Фонд ООН для развития в интересах женщин (ЮНИФЕМ), Учебный и научно-исследовательский институт ООН (ЮНИТАР), Фонд международного партнерства ООН (ФМПООН), «Глобальное партнерство в области знаний», Азиатско-тихоокеанское сообщество электросвязи, Центр по международной торговле, Франкоязычное сообщество, Консорциум по многоязычным доменным именам, Всемирный банк, региональные банки развития и многие другие организации и инициативы (по равному доступу к цифровому спутниковому вещания Программы развития ООН (ПРООН) и т. д.

Признавая все более заметную роль электронной торговли в мировом товарообороте, Целевая группа ориентирует свои усилия на поддержку инициативы ВТО по оказанию помощи развивающимся странам в развитии электронной торговли и ИКТ, которые могут возникнуть в связи с Повесткой дня ВТО в области развития, принятой в Дохе и на других торговых переговорах. В подготовленном докладе под названием «ВТО и электронная торговля: от Уругвайского раунда к Повестке дня в области развития, принятой в Дохе» рассматриваются пути преодоления препятствий и решения проблем, имеющих конкретное отношение к развивающимся странам в контексте торговли электронными товарами и услугами, с тем, чтобы они могли отстаивать на торговых переговорах свои интересы.

Благодаря сетям «диджитал диаспора», созданным Целевой группой и рядом партнеров, иностранцы, работающие в секторе высоких технологий в Северной Америке и Европе, объединяются для реализации инициатив в области ИКТ на родине. Эти сети призваны мобилизовать предпринимательский, технический и профессиональный потенциал и ресурсы различных диаспор для содействия развитию и достижению целей в этой области, поставленных в Декларации тысячелетия, за счет внедрения ИКТ. В докладах «Информационный мост в Африку» и «Информационный мост в Карибский бассейн», опубликованных в 2003 г., рассказывается о деятельности этих сетей.

5-7 мая 2003 г. в Кампале (Уганда) силами ЮНИФЕМ, ПРООН, Целевой группы по ИКТ, ФМПООН и Канцелярии Советника по особым поручениям в Африке было организовано совещание по теме «Преодоление цифрового разрыва с учетом интересов женщин», в работе которого приняли участие 150 представителей организаций системы ООН, африканских правительств, НПО, африканской диаспоры и частного сектора.

Созданная совместными усилиями Целевой группы, правительств Канады и Ирландии и Экономической комиссии для Африки (ЭКА) и представленная ими на ВВУИО, Глобальная сеть ресурсов по использованию ИКТ в области политики (ePol-NET) — это партнерское объединение, имеющее целью мобилизацию глобальных усилий на поддержку национальных стратегий использования электронных средств на благо развития. Включая в себя сетевые ресурсы заинтересованных сторон из государственного, частного и некоммерческого секторов по всему миру, ePol-NET сводит воедино источники информации и опыта в использовании электронных средств для нужд экспертов по политическим и нормативным вопросам, организаций и правительств развивающихся стран. Целевой группе удалось подключить к этой инициативе новых международных партнеров и привнести в нее региональный аспект.

2.2.1. Содействие диалогу по использованию ИКТ в целях развития

Целевая группа выступила устроителем ряда международных конференций и выпустила ряд публикаций, с тем, чтобы продвинуть дискуссии в отношении планов использования ИКТ в целях развития и дать толчок новым инициативам. Нью-йоркская серия учебных мероприятий для ознакомления с политикой и подготовки специалистов по информационным технологиям (ПАТИТ), организованная Целевой группой и ЮНИТАР в сотрудничестве с компанией «Интел» и Рабочей группой по информатике ЭКОСОС, призвана дать политикам и чиновникам из развивающихся стран базовые знания по ИКТ и смежным вопросам. В 2003 г. завершили программу, состоявшую из пяти учебных модулей, 127 участников, а примерно 315 участников посетили три семинара высокого уровня. Эта серия была продолжена в 2004 г. Глобальная программа электронного обучения для руководителей старшего звена в столицах, реализация которой начата в апреле 2004 г. после успешного тестирования, позволила охватить курсами ПАТИТ политиков по всему миру.

Целевая группа выступила соучредителем конференции Международного совета по вопросам социального обеспечения на уровне общин (МССО), посвященной вопросам облегчения доступа пожилых людей к Интернету, которая была проведена 12 февраля 2003 г. в Нью-Йорке по теме «Общины неравнодушных двадцать первого столетия: представления о возможностях».

После конференции совместными усилиями МССО, Целевой группы по ИКТ, Межамериканского банка развития и Программы ООН по населенным пунктам была выпущена публикация «Век цифровых возможностей: установление связей между поколениями». В ней излагаются различные мнения о том, каким образом ИКТ могут способствовать решению проблем, связанных со старением населения. 11 февраля 2004 г. также в ООН состоялась следующая конференция по теме «Подключение разных поколений к общей деятельности».

В ответ на призыв Генерального секретаря к предприятиям ИКТ охватить развивающиеся страны беспроводным сервисом (wi-fi) Целевая группа совместно с Институтом проблем беспроводного Интернета выступила устроителем конференции «Возможности беспроводного Интернета для развивающихся стран», которая прошла 26 июня 2003 г. в Нью-Йорке. Эта конференция послужила полезным форумом для выявления и обсуждения соответствующих проблем.

Кроме того, Институт разработал программу деятельности по итогам ВВУИО. Она предполагает проведение серии семинаров для стран арабского мира, серии семинаров для африканского континента, серии учебных занятий для работников муниципальных и местных органов власти и серии практикумов по нормативным аспектам политики использования нелицензированного диапазона частот в интересах обеспечения всеобщего доступа. Каждая серия будет включать в себя несколько практикумов и встреч в целях реализации программ создания потенциала и жизнеспособных сетей, а доклады по итогам их работы представляются на ВВУИО в Тунисе.

В качестве первого шага по осуществлению мандата, содержащегося в резолюции 57/295 Генассамблеи об использовании ИКТ в целях развития, Целевая группа по ИКТ и секретариат Совета административных руководителей по координации (САР) системы ООН организовали 24 июля 2003 г. в Женеве дискуссию, посвященную данной проблеме. В резолюции 57/295 подтверждалась необходимость использования ИКТ в качестве стратегического механизма для повышения эффективности и результативности программ в области развития и

мероприятий в области технического сотрудничества системы ООН. На основе дискуссии Генеральному секретарю были представлены предложения по общесистемной стратегии и план действий.

В 2003 г. было издано два сборника по итогам серии стратегических семинаров Целевой группы по ИКТ для послов и дипломатов. В документе «Роль ИКТ в глобальном развитии: анализ и стратегические рекомендации» собраны отдельные материалы рабочих групп Целевой группы, в которых затрагиваются проблемы, возникающие у международного сообщества, правительств и местных властей при попытках использовать ИКТ для улучшения условий жизни людей. В документе «Связь на благо развития: информационные киоски и жизнеспособность» анализируются предпосылки и важнейшие компоненты, необходимые для их успешного использования в интересах обмена идеями и передовым опытом между частными лицами и организациями, стремящимися обеспечить всеобщий доступ и охват услугами.

2.2.2. Региональные центры использования ИКТ

Вскоре после создания Целевая группа разработала на национальном, региональном и субрегиональном уровнях механизмы поощрения децентрализованного подхода к сотрудничеству на основе выявления проблем и недостатков в текущих мероприятиях по использованию ИКТ в целях развития. Основные заинтересованные стороны подключились к работе пяти тематических рабочих групп открытого состава. Региональные узлы продвижения ИКТ действуют в Африке, Азии, Латинской Америке и Карибском бассейне, арабских государствах и Европе и Центральной Азии.

2.2.2.1. Арабская региональная сеть

Сеть стремится проводить мероприятия по координации, оказанию помощи, содействию, пропаганде и просвещению, связанные с осуществлением в арабских странах проектов в области социально-экономического развития на основе использования ИКТ. Запланировано проведение ряда национальных совещаний по стратегиям использования электронных технологий, которые призваны внести вклад в разработку политики и стратегий арабских стран в сфере ИКТ.

В 2003 г. такие совещания были проведены в Иордании и Ливане. В ходе совещания в Бейруте представители национальных и

международных научных кругов, государственного и частного секторов и гражданского общества на протяжении двух дней активно выступали с заявлениями, вели прения и проводили консультации, приведшие к выработке рекомендаций, выполнение которых позволит сформировать комплексную основу, дающую правительству Ливана возможность создать благоприятные условия и адекватную инфраструктуру для того, чтобы ИКТ широко применялись в этой стране. Кроме того, была учреждена рабочая группа по региону арабских стран, которая будет координировать и отслеживать решение всех вопросов, связанных с доменными именами на арабском языке, в координации с различными арабскими и международными учреждениями и организациями, в частности Консорциумом многоязычных Интернет-имен (ИКАНН).

2.2.2.2. Африканская сеть заинтересованных сторон

Сеть является объединением, члены которого, представляющие различные области профессиональной деятельности, обмениваются информацией о крупных мероприятиях и инициативах, связанных с ИКТ, через посредство дискуссионных форумов, веб-сайтов и информационных материалов по странам. Цель этой сети, чья деятельность координируется Экономической комиссией для Африки (ЭКА), заключается в создании оптимальной общей основы для налаживания партнерских отношений и обмена ресурсами с существующими на континенте сетями по вопросам использования ИКТ в целях развития на основе результатов проводимых в настоящее время мероприятий и опыта региональных и международных учреждений, включая Партнерство в области ИКТ в Африке (ПИКТА) и Центр информационной технологии для Африки (ЦИТА).

На совещании Руководящего комитета Африканской сети 10 и 11 мая 2003 г. в Аддис-Абебе подчеркивалось ее важное значение в вопросе обеспечения проведения африканскими странами мероприятий, предусмотренных в плане действий Целевой группы по ИКТ; обмена информацией о крупных мероприятиях и инициативах; информирования, вовлечения и мобилизации основных заинтересованных сторон; обеспечения увязки соответствующих африканских и международных инициатив и программ, а также привлечения средств и инвестиций в сектор ИКТ в Африке. Африканская сеть и ее Руководящий комитет оказали значительную помощь в обеспечении вклада Африки в процесс подготовки к ВВУИО, а также в проведении в ее рамках выставки «Платформа

для использования ИКТ в целях развития». В контексте подготовки ко второму этапу ВВУИО в Тунисе начался процесс проведения консультаций в интерактивном режиме, в ходе которых основное внимание уделяется вопросам управления Интернетом.

2.2.2.3. Азиатский региональный узел

Секретариат Азиатской региональной сети был официально учрежден в январе 2003 г. в Шанхае. Находящийся в Региональном центре по вопросам сотрудничества в области информатизации городов в Шанхае секретариат оказывает основную и организационную поддержку при проведении мероприятий Целевой группы по ИКТ в регионе.

В частности, секретариат занимался организацией четвертого ежегодного Форума по вопросам информатизации городов в регионе Азии и Тихого океана, который первоначально был запланирован на июнь 2003 г., однако был перенесен на июнь 2004 г. из-за эпидемии атипичной пневмонии.

2.2.2.4. Карибско-латиноамериканский узел (LACNET)

Узел уделяет основное внимание разработке и созданию оргструктур, необходимых для реализации в регионе инициатив, связанных с использованием ИКТ в целях развития. В июне 2003 г. LACNET организовал представительный семинар с участием Председателя ВВУИО по теме «Новые модели предпринимательской деятельности: мнение частного сектора». Цель этого мероприятия заключалась в том, чтобы дать возможность представителям сектора ИКТ обсудить пути, позволяющие обеспечить рынки с более низкими уровнями дохода более дешевыми техническими средствами и программным обеспечением. LACNET также сыграл активную роль в реализации глобальной инициативы по созданию электронных школ и общин, в том числе в выборе Боливии для участия в мероприятиях в рамках первого этапа этой Инициативы. Совместно со Стэнфордским университетом, Всемирным банком и другими учреждениями он участвовал в разработке формата инициативы NetGrowth.

Сеть также внесла свой вклад в формирование Консультативного комитета расширенного состава (АЛАК) ИКАНН, который занимается созданием региональной организации расширенного состава в Латинской Америке. Латиноамериканская сеть также разработала ряд региональных проектов, связанных с электронной тор-

говлей и средними и малыми предприятиями, при поддержке Межамериканского банка развития/Многостороннего инвестиционного фонда «Программа использования ИКТ в предпринимательской деятельности».

Среди других мероприятий: создание регионального института, который занимается научно-исследовательской деятельностью и новаторскими разработками; осуществление в Карибском бассейне проекта под названием «Полностью оцифрованный остров», цель которого продемонстрировать, что благодаря внедрению беспроводных систем связи возможен полный доступ к Интернету. Обнадеживающие результаты принесли проводившиеся с несколькими компаниями частного сектора дискуссии о возможном осуществлении проектов сотрудничества, совместно с МСЭ, ИКАНН, ЮНЕСКО и другими партнерами для заинтересованных сторон этого совещание по вопросам управления Интернетом.

2.2.2.5. Московский узел региональной сети Европы и Центральной Азии

Узел действует в тесном сотрудничестве с Женевским узлом, активно участвовал в организации международной конференции по теме «Партнерские системы как инструменты активизации развития информационного общества и наукоемкой экономики» (Москва, декабрь 2002 г.). В работе этого форума участвовали 100 сотрудников директивных органов и экспертов высокого уровня из 19 стран, которые представляли правительства, деловые круги, гражданское общество, научно-исследовательские и учебные заведения, СМИ, национальные международные ассоциации и международные организации, включая Всемирный банк, ПРООН и ЕЭК ООН. Материалы конференции были широко распространены в странах СНГ и европейских странах.

Московский узел активно пропагандирует идею развития «наукоемкой экономики» в России и странах СНГ. На конференции, которая была проведена в Вильнюсе (Литва) в августе 2003 г., был представлен доклад о главных показателях для оценки готовности к развитию наукоемкой экономики, который может стать основой для разработки системы показателей, необходимых в целях подготовки национальных докладов стран Европы и Центральной Азии о развитии наукоемких технологий.

С учетом коллективного опыта, накопленного в деле реализации стратегий развития на основе использования ИКТ, Рабочая группа

по национальным и региональным стратегиям использования электронных технологий разработала предварительный план действий (10 мероприятий), который призван служить для правительств ориентиром в их деятельности и в налаживании возможного сотрудничества между заинтересованными сторонами на глобальном и национальном уровнях. Такой подход призван стимулировать реализацию стратегий использования ИКТ на национальном и региональном уровнях и обеспечить синергетический эффект, увязку, сотрудничество и координацию деятельности в рамках многочисленных нынешних и новых инициатив, осуществляемых на местах, таких, как инициативы Всемирного банка, ПРООН, Экономическая комиссия для Африки (ЭКА), МСЭ и других сторон.

Рабочая группа оказывает также поддержку реализуемым на основе сотрудничества инициативам, таким, как Глобальная сеть ресурсов по использованию ИКТ в области политики (ePol-NET), в целях создания необходимого потенциала в области развития электронных технологий путем обеспечения доступа к знаниям, информации и опыту, связанным с соответствующей политикой. В период с сентября по ноябрь 2003 г. Рабочая группа способствовала и содействовала организации серии региональных совещаний по стратегиям использования электронных технологий, которые проводились в Мапуту, (Мозамбик), Куала-Лумпуре (Малайзия) и Баку (Азербайджан). Их цель — содействовать обмену информацией и опытом в деле разработки и реализации стратегий использования ИКТ в целях развития, выявлять передовую практику деятельности и налаживать партнерские отношения между странами. На этих совещаниях также были подготовлены и приняты заявления, содержавшие рекомендации и перечень приоритетов стран и регионов, которые должны были найти свое отражение в их материалах, подготавливаемых для ВВУИО.

2.2.3. Повышение информированности населения

Рабочая группа по развитию людских ресурсов и наращиванию потенциала работает в тесном взаимодействии с соответствующими учреждениями ООН и другими партнерами из частного и государственного секторов, а также с представителями системы образования и научными работниками как в развитых, так и в развивающихся странах с целью содействия обучения пользователей ИКТ.

Особое внимание Группа уделяет следующим трем областям: развитию людских ресурсов, здравоохранению и содержанию информации.

Относительно людских ресурсов Группа уделяет особое внимание устранению неравенства между мужчинами и женщинами, в том, что касается возможностей в сфере образования и профессиональной подготовки и доступа к ним.

Одна из основных инициатив этой Группы заключалась в создании функционирующей Программы ООН «Объединения университетских добровольцев под эгидой ЮНИТЭС» (Служба информационных технологий ООН). Охваченные этой программой университеты-партнеры направляют на шестимесячный период квалифицированных, опытных добровольцев для работы в рамках проектов по созданию потенциала в области ИКТ в развивающихся странах. ЮНИТЭС получила средства от правительств Японии и Германии в целях оказания поддержки университетам стран Юга, с тем, чтобы добровольцы из университетов могли в своих собственных регионах использовать свои знания и умения в области ИКТ и вносить вклад в преодоление «цифрового разрыва» и в содействие сотрудничеству Юг—Юг.

Что касается здравоохранения, то особое внимание уделяется применению ИКТ в интересах укрепления систем и инфраструктуры в секторе медицинского обслуживания в поддержку инициативы Генерального секретаря ООН по борьбе с ВИЧ/СПИДом и другими инфекционными и заразными заболеваниями.

Рабочая группа сотрудничает с ВОЗ, Объединенной программой ООН по ВИЧ/СПИДу (ЮНЭЙДС) и ПРООН, а также с общинами, странами и национальными и международными партнерами. Проводит мероприятия по повышению уровня информированности населения, мобилизации поддержки и налаживания отношений партнерства между государственным и частным сектором в интересах удовлетворения определенных на национальном и региональном уровнях потребностей, позволяющих использовать ИКТ в таких областях, как управление и профилактика, научные исследования и разработки, лечение, распределение медикаментов, мониторинг, профессиональная подготовка и уход. Так, на Всемирной ассамблее здравоохранения 2003 г. в Женеве были представлены материалы об успешных программах использования ИКТ в секторе здравоохранения.

Подкомитет Рабочей группы, занимающийся содержанием информационных материалов для общин «Local Voices» («Местные голоса»), оказывает поддержку в деле создания материалов как для сектора образования, так и для сектора здравоохранения, которые позволяют расширить возможности малоимущих и неграмотных людей благодаря использованию ИКТ. В сотрудничестве с пред-

ставителями исполнительного секретариата ВВУИО и участниками выставки «Платформа для использования ИКТ в целях развития» Группа представила на встрече информацию о ряде мероприятий, связанных с подготовкой материалов для местных общин и использованием языков меньшинств. Для контроля за последующей деятельностью было сформировано «объединение местных голосов», цель которого заключается в распространении информации о передовых методах, определении направлений деятельности в области научных исследований и разработок и в подготовке повестки дня для второго этапа ВВУИО в Тунисе в 2005 г.

Еще одна инициатива, осуществляемая при поддержке Рабочей группы, заключалась в создании портативной системы развития базы знаний. Эта инициатива реализуется под руководством Фонда ООН в области народонаселения (ЮНФПА), который разработал функционирующую на основе Интернета систему развития базы знаний (KADS), позволяющую накапливать знания и обмениваться ими. ЮНФПА разработал «открытую» версию этой системы в сотрудничестве с университетским колледжем города Корк (Ирландия), и она была успешно представлена на ВВУИО.

2.2.4. Программы доступного подключения к Интернету

Рабочая группа по доступному подключению к Интернету стремится повысить уровень информированности населения о новых возможностях ИКТ. Эта деятельность включает поиск новых технологий подключения, а также определение новаторских деловых моделей устойчивого доступа. Было вновь подчеркнуто важное значение уделения приоритетного внимания африканскому континенту, и в повестке дня Рабочей группы одним из важных вопросов остается вопрос об оказании поддержки компоненту ИКТ в рамках Нового партнерства в интересах развития Африки (НЕПАД).

В сотрудничестве со Шведским агентством по сотрудничеству в области международного развития (СИДА) и Университетом информационных технологий Киста Рабочая группа организовала в Стокгольме 5-6 июня 2003 г. семинар по вопросам «открытого доступа». Цель семинара заключалась в определении успешных решений и стандартов для сетей, дающих открытый доступ всем («Первая миля»). Этот семинар впредь будет проводиться ежегодно.

Рабочая группа опубликовала и представила на ВВУИО документ под названием «Доступ и подключение на местах: местные решения», в котором говорилось о нетрадиционных с технической и коммерчес-

кой точек зрения методах обеспечения доступа и подключения на местах в ряде развивающихся стран. Вклад Рабочей группы в работу ВВУИО заключался еще и в том, что ее учредитель играл ведущую роль в разработке одной из пяти главных тем выставки «Платформа для использования ИКТ в целях развития» «Новаторские подходы к обеспечению доступа на справедливой основе», а также внесла свой вклад в организацию экспозиции «Сравнение различных вариантов обеспечения доступа».

Помимо этого, она мобилизовала финансовые ресурсы, которые позволили организациям гражданского общества, университетам и новаторам из развивающихся стран представить на выставке свои материалы и таким образом внести свой вклад в усилия, направленные на поиск устойчивых моделей обеспечения доступа на «первой миле». Рабочая группа также организовала на этой выставке параллельное мероприятие по теме «Открытый доступ», в ходе которого были рассмотрены различные модели обеспечения устойчивого доступа в отдаленных районах.

Рабочая группа продолжает изучать вопрос о целесообразности создания пунктов обмена информацией в Интернете и проводит работу с развивающимися странами, МСЭ и другими партнерами из государственного и частного секторов в целях создания информационной сети для повышения уровня информированности политиков об этой проблеме и координации осуществляемых в настоящее время инициатив.

Задачи Рабочей группы, связанные с политическим руководством и управлением в области ИКТ, состоят в поощрении транспарентности, легитимности и подотчетности международных процессов управления и их результатов, связанных с ИКТ, и расширении участия развивающихся стран в стратегических форумах по ИКТ. Рабочая группа выступила с предложением оказать содействие созданию африканского регионального Интернет-реестра (AfriNIC), который позволил бы расширить технические возможности для подключения, а также возможности для принятия решений совместно с ИКАНН в африканском регионе.

Рабочая группа по деловой активности и предпринимательству участвует в реализации ряда инициатив, которые нацелены на содействие развитию предпринимательства в интересах обеспечения устойчивого социально-экономического развития и смягчения остроты проблемы нищеты.

Первой из трех программ, которые осуществляются этой Рабочей группой, является программа Enablis, в рамках которой оказывается помощь тем малым, средним и мелким предприятиям в развивающихся странах, которые используют, или намереваются использовать,

электронные технологии в целях расширения своей деятельности. Первоначально она была создана рядом компаний частного сектора, участвовавших в работе Целевой группы, а в настоящее время она осуществляется под совместным руководством компаний «Аксенчер», «Ньюлет-Пакард» и «Телесистем».

Программа сотрудничает с другими организациями, которые занимаются оказанием поддержки предпринимательству, с тем, чтобы выработать комплекс взаимосвязанных мер, включая предоставление субсидий и оказание деловой и технической поддержки и консультативных услуг по вопросам стратегии, что дает малым и средним предприятиям дополнительные возможности для того, чтобы они могли успешно и на устойчивой основе осуществлять свою деятельность. В 2003 г. в Кейптауне, Южная Африка, было создано ее отделение по оперативным вопросам, и в будущем планируется создание других региональных отделений.

Вторая инициатива — «Глобальная сеть обмена информацией» (ранее называвшаяся «Сеть возможностей для развития») — позволяет наладить связь между соответствующими предпринимателями, работающими в социальной сфере, и проектами, которые осуществляются на уровне общин, в развивающихся странах с отдельными донорами, которые хотели бы предоставить им прямые взносы на безвозмездной основе. Деятельность Сети основана на убежденности в том, что гражданское общество и частный сектор, работающие в сотрудничестве с предпринимателями-представителями коренных народов и действующими на уровне общин организациями, могут внести значительный вклад в создание на коллективной основе «общественных благ» и содействовать смягчению остроты проблемы крайней нищеты. Предоставленные ресурсы использовались для финансирования проектов, связанных с привлечением учителей, владеющих двумя языками, для обучения детей представителей коренных народов в Перу; созданием в Мали предприятий по обработке бытовых сточных вод; строительством туалетов для школьников в Индии и с обучением применению информационных технологий в Непале.

Цель третьей инициативы заключается в том, чтобы найти на основе использования ИКТ решения, которые расширили бы доступ мелких предпринимателей и малых и средних предприятий в развивающихся странах к капиталу. Этот проект нацелен на налаживание эффективной связи между клиентами и занимающимися микрофинансированием учреждениями и рынками капитала путем разработки стандартов сбора и обработки данных.

2.2.5. Итоги и проблемы деятельности Целевой группы по ИКТ

Проведенный в предыдущих параграфах анализ деятельности Целевой группы ООН по ИКТ за 2003–2005 гг. убедительно демонстрирует как ее эффективность, так и слабые стороны.

Работу Группы затрудняет ограниченность ресурсов и тот факт, что ее возможности в плане активного налаживания сотрудничества и принятия на себя ответственности за создание в странах благоприятных условий для развития ИКТ и для их экономического развития зависят от правительств самих стран. Целевая группа по ИКТ доказала, что она может вносить заметный вклад в решение вопросов развития, обеспечивать активное участие политиков в дискуссиях по вопросам ИКТ, выявлять узкие места в программах и возможности для обеспечения взаимодействия между заинтересованными сторонами и стимулировать принятие мер и координировать осуществление мероприятий на основе сотрудничества. Она помогла разработать новые модели руководства и сотрудничества в деле активизации глобальных усилий по преодолению «цифрового разрыва» и созданию равных возможностей в информационной области для всех. По сути, этот орган создал организационную инфраструктуру, в рамках которой можно использовать ИКТ в целях искоренения нищеты и создания новых возможностей для всех людей во всем мире. Главное внимание в контексте этих усилий по-прежнему уделяется развивающимся странам, в особенности странам Африки и наименее развитым странам.

Проблемы, с которыми сталкивается Целевая группа, известны. Обстановка в мире является чрезвычайно сложной, а это означает, что необходимо оперативно адаптироваться к изменениям. После периода значительного сокращения объема средств начался процесс возобновления предоставления финансовых ресурсов. В конечном счете, эффективное использование ИКТ в целях развития в будущем будет зависеть от приверженности правительств принципам успешного управления, защиты прав человека, рациональным экономическим стратегиям и борьбе с коррупцией и за верховенство закона. Кроме того, оно зависит от формирования благоприятных условий в политической и организационной областях, способствующих привлечению инвестиций, необходимых для использования ИКТ в целях развития.

Эффективность работы Целевой группы также зависит от обеспечения участия в ее работе ключевых институтов и заинтересованных сторон на постоянной основе. Преодоление «цифрового разрыва» и предоставление доступа всем связаны с решением комплекса вопро-

сов, таких, как создание инфраструктуры, внедрение технических новшеств, инвестиций, образования и профессиональной подготовки, а также содержания информационных материалов. В этом контексте решающее значение имеет интеграция стратегий развития ИКТ в общие национальные стратегии развития.

На основе опыта, накопленного на протяжении 2003 г., на 2004–2005 гг. были выделены следующие пять приоритетных направлений:

- обеспечение увязки между ИКТ и согласованными на международном уровне целями в области развития, включая цели, закрепленные в Декларации тысячелетия;
- налаживание партнерских отношений между многочисленными заинтересованными сторонами;
- решение проблем политики и управления в области ИКТ;
- содействие созданию благоприятных условий.
- подготовка к проведению второго этапа ВВУИО в Тунисе (ноябрь, 2005).

2.3. От Хартии глобального информационного общества «восьмерки» (Окинава, 2000 г.) к Всемирной встрече на высшем уровне по информационному обществу (Женева, 2003 — Тунис, 2005)

«Большая семерка», а затем и «восьмерка» во взаимодействии с ООН, ВТО, ОЭСР и другими международными структурами последнее десятилетие постоянно держит в поле зрения проблематику ИКТ. По оценке экспертов наиболее важным документом стала Хартия глобального информационного общества, принятая на саммите «восьмерки» на Окинаве. Однако для лучшего понимания Хартии представляется оправданным рассмотреть материалы конференции «семерки», проходившей с 24 по 26 февраля 1995 г. в Брюсселе[11].

2.3.1. Конференция G7 в Брюсселе (1995 г.)

В документах конференции было подчеркнуто, что ИКТ производят новую революцию, которая вводит человечество в ГИО и воздействует не только на взаимодействие людей, но и на государственные структуры. Традиционно жесткие и застывшие, они подлежат замене

[11] G-7 Ministerial Conference on the Information Society, Brussels, 1995 — http://www.ispo.cec.be/g7/

более гибкими, децентрализованными моделями, что, в конечном итоге, преобразует общество, функционирование экономики, частный бизнес и государственные институты. Создание ГИО определялось одной из наиболее важных инициатив, которые необходимо предпринять в кратчайшие сроки. Были обозначены следующие потенциальные преимущества от этого: более высокий уровень социальной интеграции, восстановление чувства сообщества, сохранение и распространение культуры, стимулирование закрепления и дальнейшего развития демократических ценностей, более высокая экономическая эффективность, установление баланса между нациями в социальном и экономическом прогрессе, гармоничная интеграция развивающихся стран в глобальную экономику[12].

При этом конкуренция должна проходить в равных условиях для всех стран. Еще в ноябре 1994 г. среди членов ЕС был достигнут консенсус по вопросу полной либерализации телекоммуникационной инфраструктуры и рынка соответствующих услуг к 1 января 1998 г. В результате большинство стран «семерки» уже практически либерализовали сектор мобильных, спутниковых и прочих телекоммуникационных услуг, кроме телефонии. Некоторые страны значительно продвинулись и в этой области[13].

Результатом Брюссельской конференции стали одиннадцать пилотных проектов ГИО:

1. Проект мировой переписи (электронно-доступный мультимедийный перечень информации, относящийся к национальным и международным проектам и исследованиям по развитию ГИО). Ответственный: Евросоюз и Япония;
2. Глобальная совместимость высокоскоростных сетей (организация международных связей между различными высокоскоростными сетями). Ответственный: Канада и Япония;
3. Интернациональное (кросс-культурное) образование и обучение (инновационные подходы к изучению языков, особенно для студентов и представителей малого бизнеса). Ответственный: Франция и Германия;
4. Электронные библиотеки (распределенная коллекция знаний человечества, доступная большинству членов общества через сети). Ответственный: Франция и Япония;

---

[12] Annual Report of the European Commission, 1995. — http://www.ispo.cec.be

[13] *Смолян Г.Л., Черешкин Д.С.* Информационно-коммуникационная инфраструктура — технологический фундамент информационного общества // Информационное общество. 1999. № 5. С. 51-53.

5. Мультимедийный доступ к мировому культурному наследию (электронные музеи и галереи). Ответственный: Италия и Франция;

6. Окружающая среда и контроль состояния природных ресурсов (электронные информационные ресурсы по этим вопросам). Ответственный: Канада;

7. Глобальное управление чрезвычайными ситуациями (информационная сеть для управления ситуациями, связанными с чрезвычайными мерами и рисками). Ответственный: США;

8. Мировая система здравоохранения (телемедицина). Ответственный: Европейская комиссия;

9. Электронное правительство (использование новых ИКТ для осуществления административной деятельности и взаимодействия в режиме он-лайн между органами исполнительной власти, юридическими лицами и гражданами). Ответственный: Великобритания;

10. Глобальный рынок для среднего и малого бизнеса (развитие среды открытого и свободного обмена информацией и предоставления глобальных торговых услуг в интересах среднего и малого бизнеса). Ответственный: Европейская комиссия, Япония, США;

11. Морские информационные системы (повышение конкурентоспособности всех морских видов деятельности за счет ИКТ). Ответственный: Европейская комиссия, Канада.

Особого внимания заслуживает проект глобальной переписи (Global Inventory Project, GIP). Программа представляет собой мультимедийную опись всех существующих национальных и международных проектов, относящихся к ГИО. Однако GIP не следует воспринимать как «просто опись», или простой перечень проектов. Действительно, это информационная система, хранящая данные о проектах и их разработчиках, но в удобной, комфортной для пользователя диалоговой среде. Таким образом, представляя общие, весьма гибкие средства поиска и обеспечения диалога на многих языках, этот глобальный интерфейс, основанный на национальных и международных инициативах, увеличивает саму ценность информации и данных, собираемых с членов-участников[14].

Итогом конференции в Брюсселе стало не только определение проектов и общих принципов, которыми следует руководствоваться в развитии ГИО, но и выработка путей их реализации. К ним относятся:

- развитие глобальных рынков для компьютерных сетей и различных ИКТ-услуг;

[14] Проекты G7 — http://www.ispo.cec.be/g7/rojects/g7pr4.html

- обеспечение технической возможности соединения и оперирования этих сетей, сотрудничество в области исследований и разработок по созданию новых ИКТ, продуктов и услуг;
- обеспечение информационной безопасности личности и данных;
- отслеживание и последующий анализ социальных последствий развития информационного общества.

2.3.2. Актуальные аспекты Окинавской Хартии глобального информационного общества

Результаты выполнения решений конференции «семерки» в Брюсселе были обсуждены на саммите «восьмерки» 22 июля 2000 года на Окинаве, где также была принята и Хартия ГИО. В ходе саммита были вновь подтверждены огромные возможности ИКТ для решения разного рода экономических и социальных проблем. Вместе с тем, было подчеркнуто, что беспрецедентное ускорение информационно-технологических процессов не только закрепляет существующий разрыв между странами т.н. «золотого миллиарда» и остальным миром, но и с каждым днем значительно его увеличивает.

Подобное положение дел вызывает серьезные опасения, в частности у лидеров стран «Большой восьмерки», которые считают, что каждый человек должен иметь возможность пользоваться теми благами, которые предоставляет глобальное информационное общество. Подчеркивая необходимость сокращения разрыва в доступе к ИКТ между развитыми и развивающимися странами, участники саммита выразили уверенность, что солидная основа политики и действий в информационной сфере способна изменить методы взаимодействия стран по продвижению социального и экономического прогресса во всем мире. Было также отмечено, что эффективное партнерство среди участников, включая совместное политическое сотрудничество, является одним из ключевых элементов рационального развития информационного общества. При этом главная задача заключается не только в стимулировании и содействии переходу к информационному обществу, но также и в полной реализации его экономических, социальных и культурных преимуществ. Для достижения этих целей были определены следующие направления работы:

- проведение экономических и структурных реформ в целях создания обстановки открытости, эффективности, конкуренции и использования нововведений, которые дополнялись бы мерами по

адаптации на рынках труда, развитию людских ресурсов и обеспечению социального согласия;

- рациональное управление макроэкономикой, способствующее более точному планированию со стороны деловых кругов и потребителей, и использование преимуществ ИКТ;
- разработка информационных сетей, обеспечивающих быстрый, надежный, безопасный и экономичный доступ с помощью конкурентных рыночных условий и соответствующих нововведений к сетевым технологиям, их обслуживанию и применению;
- развитие людских ресурсов, способных отвечать требованиям века информации посредством образования и пожизненного обучения, и удовлетворение растущего спроса на специалистов в области ИКТ во многих секторах экономики;
- активное использование ИКТ в государственном секторе и содействие предоставлению в режиме реального времени услуг, необходимых для повышения уровня доступности власти для всех граждан[15].

Было признано, что частный сектор играет существенную роль в разработке ИКТ, формировании и развитии ГИО в целом. Однако задача создания предсказуемой и недискриминационной политики и нормативной базы, необходимой для ГИО, лежит на правительствах. В частности, необходимо, чтобы правила и процедуры, имеющие отношение к ИКТ, соответствовали коренным изменениям в экономических сделках с учетом принципов эффективного партнерства между государствами и частным сектором. В целях максимизации социально-экономической выгоды ГИО участники саммита согласились со следующими основными принципами и подходами и рекомендовали их другим странам:

- продолжение содействия развитию конкуренции и открытию рынков для ИКТ, продукции и услуг, включая недискриминационное и основанное на затратах подключение к основных телекоммуникациям;
- защита прав интеллектуальной собственности на ИКТ имеет особое значение для продвижения нововведений, связанных с ними, развития конкуренции и внедрения новых технологий; важно вновь подтвердить обязательство правительств использовать только лицензированное программное обеспечение;
- ряд услуг, включая телекоммуникации, транспорт, доставку

[15] Окинавская Хартия глобального информационного общества // Дипломатический вестник. 2000. № 8. С. 52.

посылок, имеют принципиальное значение для ГИО и экономики; повышение их эффективности и конкурентоспособности позволит расширить преимущества ГИО; таможенные и экспедиторские процедуры также важны для развития информационных структур;

- развитие трансграничной электронной торговли путем содействия дальнейшей либерализации, улучшение сетей и соответствующих услуг и процедур в контексте жестких рамок ВТО, продолжение работы в области электронной торговли в ВТО и на других международных форумах и применение существующих торговых правил ВТО к электронной торговле;
- последовательные подходы к налогообложению электронной торговли, основанные на обычных принципах, включая отсутствие дискриминации, равноправие, упрощенность и прочие элементы, согласованные в контексте работы Организации экономического сотрудничества и развития (ОЭСР);
- продолжение практики освобождения электронных переводов от таможенных пошлин до тех пор, пока она не будет рассмотрена вновь на следующей министерской конференции ВТО;
- продолжение рыночных стандартов, включая, например, технические стандарты функциональной совместимости;
- повышение доверия потребителя к электронным рынкам в соответствии с руководящими принципами ОЭСР, в том числе посредством эффективных саморегулирующих инициатив, таких как кодексы поведения, маркировка, другие программы подтверждения надежности, и изучение вариантов устранения сложностей, которые испытывают потребители в ходе трансграничных споров, включая использование альтернативных механизмов разрешения споров;
- развитие эффективного и значимого механизма защиты частной жизни потребителя, а также защиты частной жизни при обработке личных данных, обеспечивая при этом свободный поток информации;
- дальнейшее развитие и эффективное функционирование электронной идентификации, электронной подписи, криптографии и других средств обеспечения безопасности и достоверности операций[16].

Участники саммита выразили уверенность в том, что усилия международного сообщества, направленные на развитие ГИО, должны сопровождаться согласованными действиями по созданию безопас-

[16] Окинавская Хартия глобального информационного общества // Дипломатический вестник. 2000. № 8. С. 53.

ного и свободного от преступности киберпространства. Было принято решение расширить сотрудничество стран «Большой восьмерки» в рамках Лионской группы по транснациональной организованной преступности. Подчеркивалась также необходимость найти эффективные политические решения таких актуальных проблем, как, например, несанкционированный доступ и компьютерные вирусы.

Важное место в дискуссиях занял вопрос о преодолении цифрового разрыва внутри государств и между ними. Для рассмотрения и выработки более широкого международного подхода к решению проблемы равного доступа к ИКТ на саммите было принято решение об учреждении Группы по возможностям информационных технологий (Digital Opportunities Task Force, DOT Force). В нее вошли по три представителя государства, бизнеса и гражданского общества от каждой из стран G8, а также представители развивающихся стран и стран с переходной экономикой[17].

Ее задачи — активно содействовать диалогу с развивающими странами, международными организациями и другими участниками для продвижения международного сотрудничества с целью формирования политического, нормативного и сетевого обеспечения, а также улучшения технической совместимости, расширения доступа, снижения затрат, укрепления человеческого потенциала; поощрять усилия «восьмерки» в осуществлении экспериментальных программ и проектов в области ИКТ и содействовать более тесному политическому диалогу между партнерами, а также более интенсивно работать над тем, чтобы мировая общественность больше знала о стоящих перед ней вызовах и имеющихся возможностях.

Для выполнения этих задач Группой были разработаны варианты принятия конкретных мер в следующих приоритетных областях:

формирование политического, нормативного и сетевого обеспечения:

- поддержка политического консультирования и укрепление местного потенциала с тем, чтобы способствовать проведению направленной на создание конкуренции гибкой и учитывающей социальные аспекты политики, а также нормативному обеспечению;
- содействие обмену опытом между развивающимися странами-партнерами, более эффективному и широкому использованию

[17] От России в состав совета вошли: от государства — О.В. Плаксин (Администрация Президента РФ), от бизнеса — И.Р.Агамирзян (Майкрософт Россия), от организаций гражданского общества — М.В.Якушев (Институт развития информационного общества и Союз операторов Интернет).

ИКТ в области развития, включая такие направления, как сокращение бедности, образование, здравоохранение и другие, не менее важные;

- совершенствование системы управления, включая изучение новых методов комплексной разработки политики, а также поддержка усилий МБР и других международных организаций в целях объединения интеллектуальных и финансовых ресурсов в контексте всевозможных программ сотрудничества;
- улучшение технической совместимости, расширение доступа и снижение затрат;
- мобилизация ресурсов в целях улучшения информационно-коммуникационной инфраструктуры, уделение особого внимания партнерскому подходу со стороны правительств, международных организаций и частного сектора;
- поиск путей снижения затрат для развивающихся стран в обеспечении технической совместимости;
- поддержка программ доступа на местном уровне;
- поощрение технологических исследований и прикладных разработок в соответствии с конкретными потребностями развивающихся стран, а также производства современной информационно содержательной продукции, включая расширения объема информации на родных языках;

укрепление человеческого потенциала:

- уделение повышенного внимания базовому образованию, расширение возможностей пожизненного обучения с упором на развитие навыков использования ИКТ;
- содействие подготовке специалистов в сфере ИКТ и других актуальных областях, а также в нормативной сфере;
- разработка инновационных подходов в целях расширения традиционной технической помощи, включая дистанционное обучение и подготовку на местном уровне;

поощрение участия в работе глобальных сетей электронной торговли:

- оценка и расширение возможностей использования электронной торговли посредством консультирования при открытии бизнеса в развивающихся странах, а также путем мобилизации ресурсов в целях содействия предпринимателям в использовании ИКТ для повышения эффективности их деятельности и расширения доступа к новым рынкам;
- обеспечение соответствия возникающих «правил игры» усилиям в сфере развития и укрепления способности развиваю-

щихся стран играть конструктивную роль в определении этих правил[18].

Рассмотрение проблемы «цифрового разрыва» между высокоразвитыми и развивающимися странами заняло свое место в повестке дня и практически всех последующих встреч лидеров стран «Большой восьмерки». Особо следует выделить саммит G8 в Генуе 20-22 июля 2001 г., где был подписан план действий, подготовленный Группой по возможностям информационных технологий (DOT Force), которая была создана на саммите в Окинаве.

План призван ликвидировать так называемое «цифровое неравенство», которое, как было отмечено, становится все более очевидным как на национальном, так и на международном уровне. План предусматривает, в частности, разработку национальных стратегий в области новых ИКТ для развивающихся стран. Эти «электронные» стратегии должны стать основой глобальной политики, направленной на развитие новых технологий в каждой стране, в том числе правительственных инициатив в области электронных систем и средств связи, а также на повышение конкурентоспособности в целом. Однако следует отметить, что успешность и сроки реализации этого и других подобных планов и программ зависят не только от активности стран-лидеров в области новых технологий, но и, в первую очередь, от самих развивающихся стран: сумеют ли они воспользоваться предоставленным информационной революцией уникальным шансом для необходимого прорыва.

По оценкам многих экспертов, несмотря на то, что проблематика ГИО рассматривалась практически на всех саммитах «восьмерки», а также на иных представительных форумах, Окинавская Хартия глобального информационного общества стала своего рода его международной конституцией.

2.3.3.Первый этап Всемирной встречи на высшем уровне по информационному обществу (ВВУИО)

По мнению ряда экспертов, «первый кирпич» в фундамент ВВУИО был заложен в опубликованном еще в 1984 г. докладе МСЭ под названием «Отсутствующее звено». В нем говорилось об огромной пропасти в сфере телекоммуникации между странами с формирующейся

[18] Там же. С. 55-56.

экономикой и развитыми странами и признавалось, что связь является важнейшим средством всеобщего повышения качества жизни. Затем данная проблема постоянно присутствовала практически на всех конференциях МСЭ.

На состоявшейся в 1998 г. в Миннеаполисе (США) конференции МСЭ была одобрена инициатива Туниса о созыве ВВУИО. В принятой резолюции 73 было рекомендовано Генеральному секретарю МСЭ внести вопрос о проведении ВВУИО в повестку дня Административного комитета по координации ООН и сообщить Исполнительному совету МСЭ о результатах консультаций. В докладе по результатам консультаций на очередной сессии Исполнительного совета в 1999 г. Генеральный секретарь МСЭ проинформировал, что ВВУИО будет проведена под патронажем Генерального секретаря ООН, а МСЭ будет играть главную роль в подготовке встречи в сотрудничестве с заинтересованными учреждениями ООН и другими международными организациями и принимающими странами. В июне 2001 г. Совет МСЭ принял решение о проведении первого этапа ВВУИО в Женеве 10-12 декабря 2003 г. и второго — в Тунисе в 2005 г.

В декабре 2001 г. ГА ООН одобрила консенсусом резолюцию 56/183 о созыве ВВУИО, которая определила основные организационные аспекты процесса подготовки к этому крупнейшему международному форуму. Проработка повестки дня встречи, проектов ее итоговых документов и правил процедуры была возложена на межправительственный Подготовительный комитет (ПК) открытого состава. Резолюция предлагала правительствам обеспечить как можно более высокий уровень своего представительства.

Первое заседание ПК состоялось в Женеве 1-5 июля 2002 г. В ходе возникшей дискуссии окончательно договориться по перечню и сформировать повестку дня ВВУИО не удалось, однако был достигнут консенсус по процедурным вопросам для подготовительных мероприятий. При этом, несмотря на доводы о том, что бизнес и гражданское общество должны быть активными участниками формирования ГИО, ряд развитых стран не добился участия их представителей из частного сектора в процессе межправительственных переговоров. Главным аргументом против их позиции стало то, что по итогам переговоров обязательства возьмут на себя государства, а не деловые круги и неправительственные организации[19].

[19] См. Крутских А.В., Крамаренко Г.И. Дипломатия и информационно-коммуникационная революция // Международная жизнь. 2003. № 7.

Важную роль в подготовке саммита сыграли региональные конференции, проводившиеся под эгидой региональных центров Целевой группы по ИКТ ООН. Эти конференции определили подходы стран соответствующих регионов к формированию ГИО с учетом их собственных интересов, потребностей и приоритетов и внесли предложения к проектам итоговых документов саммита.

В рамках процесса подготовки к встрече в период между первой и второй сессиями ПК состоялось пять региональных конференций и две субрегиональные. Эти международные форумы явились крупными политическими событиями для стран соответствующих регионов.

Так, представители правительств, деловых и научных кругов, а также гражданского общества из десяти стран, главным образом СНГ, участвовавшие в субрегиональной Бишкекско-московской конференции по ГИО, постановили в центр внимания человека со всем многообразием его интересов, сохранение культурного и лингвистического разнообразия информационного общества, учет специфического географического положения стран субрегиона, дальнейшее развитие научных исследований и подготовку квалифицированных кадров в области ИКТ, а также привлечение инвестиций в регион.

В Общеевропейской и в Азиатско-тихоокеанской региональных конференциях по подготовке к ВВУИО приняли участие делегации 47 стран, представители международных организаций, частного сектора и гражданского общества. Принятые на них итоговые документы в значительной степени базируются на идеологии Окинавской хартии ГИО. Вместе с тем в Токийской декларации более широко, чем в Бухарестской, представлен социальный аспект ГИО, большее внимание уделено преодолению «цифрового разрыва», оказанию помощи развивающимся странам.

На марракешской (2002 г.) конференции МСЭ подготовка к ВВУИО стала одним из главных вопросов повестки дня. Конференция одобрила предложения («вклад») МСЭ к проектам итоговых документов ВВУИО, которые направлены на достижение следующих основных целей:

- обеспечение доступа к ИКТ для всех;
- ИКТ должны стать инструментом экономического и социального развития и достижения «целей тысячелетия» в области развития, зафиксированных в Декларации тысячелетия ООН;
- доверие и безопасность при использовании ИКТ.

На второй сессии Подготовительного комитета ВВУИО, состоявшейся в Женеве 17-28 февраля 2003 г., проекты итоговых документов саммита вновь не были одобрены, в том числе по причине попыток ряда

развитых стран добиться участия неправительственного сектора в переговорах, а развивающихся стран — закрепить за собой ведущую роль в подготовке проектов документов. Развитые страны вынудили участников согласиться на включение в один сводный документ предложений государств и неправительственного сектора. Переговоры были продолжены на заседании редакционной группы открытого состава в Париже в июле 2003 г. и на третьей сессии ПК (Женева, 15-26 мая 2003 г.).

Наряду с сессией ПК, перед ВВУИО в Женеве состоялись другие важные мероприятия, в том числе под эгидой Генерального секретаря ЮНЕСКО К.Мацууры прошел симпозиум на тему «Общество знаний — от видения к действию»[20].

В первом этапе ВВУИО (Женева, 10-12 декабря 2003 г.) приняли участие более 60 глав государств и правительств, в основном из развивающихся стран. Развитые страны были представлены главным образом на уровне министров по вопросам связи и информатизации. Всего в ВВУИО участвовало более 11 тысяч человек, представлявших государственные структуры, деловые круги и гражданское общество из 176 стран мира, а также заинтересованные международные организации. В своем вступительном слое Генеральный секретарь ООН К.Аннан особо подчеркнул: «Эта встреча на высшем уровне является уникальной. В то время как большая часть глобальных конференций посвящена глобальным угрозам, на этой будет рассмотрен вопрос о том, как лучшим образом использовать новое глобальное достояние».

Россию на ВВУИО в соответствии с распоряжением Правительства представляла делегация под руководством министра по связи и информатизации Л.Д. Реймана. В ее состав вошли представители заинтересованных министерств и ведомств (МИД России представлял зам. министра Кисляк С.И.), а в качестве экспертов — представители государственных структур, бизнеса, гражданского общества и научных организаций.

Руководитель российской делегации был избран сопредседателем ВВУИО и был одним из председателей первого пленарного заседания встречи. В своем выступлении он отметил важность развития и использования ИКТ в различных сферах деятельности, приоритетность создания инфраструктуры, обеспечения доступа широких слоев населения к информационным ресурсам и услугам, сокращения «цифрового разрыва».

---

[20] http://portal.unesco.org/ci/en/ev.php-URL_ID=10588&URL_DO=DO_-TOPIC&URL_SECTION=201.html

Итогом ВВУИО стало принятие на основе консенсуса двух документов — «Декларации принципов построения информационного общества: глобальный вызов в новом тысячелетии» и «Плана действий», в которых в полной мере нашли отражение российские предложения.

Данные результаты достигнуты в ходе длительных переговоров и поиска компромисса между развитыми и развивающимися странами, а также интересами государственного сектора, делового сообщества и неправительственных организаций по ряду основополагающих вопросов, касающихся формирования ГИО.

В итоговых документах ВВУИО отмечается важность развития инфраструктуры как необходимой основы для предоставления населению доступа к ИКТ. Предусматривается развитие и укрепление инфраструктуры национальных, региональных и международных сетей широкополосной связи, включая спутниковые и другие системы, для предоставления новых услуг на основе ИКТ.

В документах ВВУИО нашли отражение современные тенденции интеграции ИКТ и технологий интерактивного вещания. В документах ВВУИО отмечено, что при использовании ИКТ должны соблюдаться общепризнанные права человека и принцип свободы доступа к информации. Участники ВВУИО призвали СМИ к ответственному использованию информации и ее подаче в соответствии со стандартами профессиональной этики.

Одним из наиболее сложных на ВВУИО стал вопрос финансирования деятельности по преодолению разрыва в использовании цифровых технологий. В итоге удалось сформулировать компромиссный текст, предусматривающий формирование добровольного «Фонда цифровой солидарности», создания которого добивались развивающиеся государства. 1 июля 2004 г. была учреждена Целевая группа под эгидой Генерального секретаря ООН по анализу ныне действующих механизмов финансирования и их соответствия задачам, возникающим в результате внедрения ИКТ для целей развития.

Принятые на ВВУИО Декларация принципов и План действий предусматривают, в частности, подключение к Интернету 2015 году всех деревень, учебных заведений, медицинских центров, больниц и местных отделений и департаментов центрального правительства. К числу других целей относится включение в учебные планы всех средних школ компонента ИКТ и обеспечение к указанному сроку всеобщего доступа к телевидению и радио. В этой же связи предлагаются меры

по распространению выгод от ИКТ на весь мир и защите конфиденциальности и обеспечению свободы прессы, которые будут включать усилия по:

- созданию интерактивного медицинского портала для обмена данными между странами с низким и высоким уровнями доходов;
- созданию систем прогнозирования стихийных бедствий[21] и антропогенных катастроф, контроля за последствиями для окружающей среды и разработки проектов по экологически безопасному удалению и утилизации аппаратных средств;
- установлению партнерских отношений для обмена информацией по сельскому, рыбному и лесному хозяйству и продовольственной промышленности;
- снижению налогов на аппаратные средства и программное обеспечение и распространение информации о программном обеспечении с открытым кодом;
- созданию всемирного библиотечного портала и открытого архива научной информации;
- поощрению предоставления консультативных услуг по вопросам микрофинансирования и торговли;
- организации круглых столов с участием доноров;
- разработке гарантий компьютерной безопасности с уделением основного внимания банкам в плане надежности компьютерных сделок;
- содействию странам в разработке законодательства по вопросам безопасности ИКТ и учреждении координационных центров для урегулирования инцидентов и принятия ответных мер в реальном времени и созданию совместной сети для обмена информацией;
- расширению исследований по созданию устройств для общественного подключения к Интернету стоимостью до 100 долл. США и для сельской местности.

Как уже отмечалось, в Целевой группе ООН по ИКТ представлены самые разнообразные заинтересованные стороны, у нее в наличии глобальная система вспомогательных органов и сетей, что дало ей уникальную возможность оказывать поддержку чрезвычайно важным мероприятиям по выработке и осуществлению решений ВВУИО. Решение о продлении срока действия ее мандата до декабря 2005 г., т.е. до завершения этапа ВВУИО в Тунисе подтверждает данный тезис.

[21] Приобрело особую актуальность после чудовищного землетрясения и цунами в Азии в декабре 2004 г.

2.3.4. Глобальный форум по регулированию Интернета (2004 г.)

Принимая во внимание то обстоятельство, что на ВВУИО больше всего противоречий вызвал вопрос о регулировании Интернета, Целевая группа по ИКТ выступила инициатором проведения 26 марта 2004 г. глобального форума по данной проблеме. Выступая на открытии форума, Генеральный секретарь ООН К.Аннан подчеркнул, что «перед нами стоят многочисленные и сложные проблемы». Действительно, среди экспертов нет даже единого мнения по определению понятия «регулирование Интернета», однако большинство понимает, что обеспечение надежности и безопасности этого пространства — в интересах всего мира. Не менее важным является создание всеобъемлющих и совместных моделей регулирования, т.к. в настоящее время охват Интернетом крайне неравномерен (подробнее см. 2.1.2) и огромное количество людей все еще лишены тех преимуществ, которые он дает, или вовсе не знакомо с ними.

По итогам дискуссий Генеральный секретарь создал соответствующую рабочую группу с небольшим секретариатом, пообещав, что ее работа будет открытой, транспарентной и всеобъемлющей по отношению ко всем сторонам. Принимая во внимание Глобальную инициативу по созданию электронных школ и общин, начало которой было положено на ВВУИО, Целевая группа по ИКТ при поддержке специально созданного секретариата, базирующегося в Ирландии, реализовала этот проект в Боливии, Гане, Индии и Намибии. В 2006 г. начнется осуществление этой инициативы в следующей группе стран.

В течение 2005 г. продолжается принятая на ВВУИО масштабная программа Института проблем беспроводного Интернета, включающая систему обучения.

Как показал эксперимент в Индии, оперативный доступ к удаленным районам с помощью сети Интернет содействует улучшению жизни в этих районах стран. Так, Интернет-киоск «n-Logue», стоимостью в 1000 долларов позволяет оперативно диагностировать эпидемии и заболевания посевов и лечить их в удаленных деревнях с помощью электронной почты и видеоконференций при доходах в 2,5 доллара в день. В настоящее время в Индии распространено около 950 000 таких киосков, которые генерируют четверть всех поступлений от телесвязи.

Возможности Интернета поистине впечатляют. 12 сентября 2004 г. достигнут новый рекорд скорости передачи данных по наземным каналам связи в сети общего пользования Internet 2. Скорость 4,31 Гбит/с

поддерживалась на расстоянии почти в 29 тыс. км. Предыдущий рекорд передачи данных по наземным каналам связи был установлен 28 мая 2004 г. Тогда по участку оптоволокна, который соединяет Калифорнийский технологический институт (Caltech) в Лос-Анджелесе и CERN в Женеве (15776 км), было передано примерно 849 ГБ данных за 600 секунд, что соответствует 103 583 Пбитм/с (петабит-метров в секунду)[22].

Гигабитный Интернет ждет нас и в сетях четвертого поколения (4G) сотовой связи, которую разрабатывает японский телекоммуникационный гигант NTT DoCoMo, Inc. Экспериментальный фрагмент сети использует радиоинтерфейс на основе технологии VSF-Spread OFDM и MIMO-модулирование сигнала, позволяющее достичь скорости в 1 Гбит/с в полосе 100 МГц. Ожидается, что первые коммерческие сети сотовой связи четвертого поколения появятся в Японии уже к 2010 г.

Интернет технологии развиваются динамично и многопланово и их роль в развитии человечества резко возрастает[23]. В силу этого, достигнутые на форуме договоренности, несомненно, станут одними из центральных на тунисском этапе ВВУИО.

2.3.5. На пути ко второму этапу ВВУИО (Тунис, 2005 г.)

26 июня 2004 г. в Хаммамете завершил работу первый Подготовительный комитет Тунисского этапа ВВУИО. На встрече были приняты общие решения по вопросам, которые будут в центре внимания Тунисского саммита. Также были достигнуты договоренности о структуре второго этапа подготовительного процесса.

В задачи первого Подготовительного комитета входило определить:

- проблемы информационного общества, которые должны рассматриваться на Тунисском саммите;
- характер тех итогов, которыми должен завершиться Тунисский саммит;
- пути достижения целей, которые были заявлены в Женевском Плане действий;

Достигнуто понимание, что центральной темой подготовительного процесса должны стать два вопроса: с одной стороны, он должен помочь найти решения вопросам реализации и развития решений,

[22] http://www.webplanet.ru/news/internet/2004/10/4/internet2.html

[23] http://www.isoc.org/isoc/reports/ar2003/annualreport.txt

принятых в Женеве (Декларации принципов и Плана действий) заинтересованными лицами на национальном, региональном и международном уровнях. При этом особое вниманием должно быть уделено тем вызовам, с которыми сталкиваются наименее развитые страны. С другой стороны, подготовительный процесс должен помочь завершить проект по управлению и финансированию Интернета, который был разработан в Женеве. Доклад целевой группы по механизмам финансирования и доклад рабочей группы по управлению Интернетом будут особенно полезны при проведении дискуссии. *Было также решено, что соглашения, достигнутые в Женеве, больше не должны становиться предметом дискуссий.*

С учетом трудностей с финансированием саммита кампания по сбору средств для ВВУИО была начата в апреле 2004 г. Во время Хаммаметской встречи было объявлено, что сумма финансовых пожертвований составляет 907 000 швейцарских франков, а общая сумма Фонда составит примерно 1,3 миллиона франков, что составляет 26% от запланированной конечной суммы в 5 миллионов франков. Общие затраты на организацию основных мероприятий подготовительного процесса и саммита в Тунисском этапе оцениваются примерно в 15 миллионов швейцарских франков, что не включает затрат принимающей страны.

Вторая встреча Подготовительного комитета ВВУИО состоялась в Женеве с 17 по 25 февраля 2005 г.

2.3.6. Вторая Бишкекско-Московская региональная конференция по информационному обществу (Бишкекский этап)

16-18 ноября 2004 г., ровно за год до начала тунисского этапа ВВУИО, состоялся первый этап Второй Бишкекско-Московской конференции по информационному обществу в рамках подготовки к саммиту стран — участников Регионального содружества в области связи (РСС). Второй этап Конференции состоится в Москве в первой половине 2005 г.

В Конференции приняли участие представители Азербайджанской Республики, Республики Казахстан, Кыргызской Республики, Республики Молдова, Российской Федерации, Республики Таджикистан, Европейской экономической комиссии ООН (ЕЭК), Экономической и социальной комиссии Азии и Тихого океана ООН (ЭСКАТО), Программы развития ООН (ПРООН), а также представители деловых кругов и гражданского общества региона.

В ходе Конференции обсуждены вопросы формирования консолидированной позиции стран СНГ по вопросам повестки дня второго этапа ВВУИО:

- вклад в развитие информационного общества;
- региональное и межрегиональное сотрудничество в ИКТ для развития;
- наращивание потенциала для применения ИКТ.

В принятой на конференции резолюции отмечено:

- внедрение ИКТ в регионе происходит быстрыми темпами, развитие сферы ИКТ является одним из приоритетных направлений во многих странах СНГ;
- ИКТ находят все более широкое применение в области государственного управления, экономике и социальной сфере (электронное правительство, электронная экономика, электронное здравоохранение, электронное образование и др.);
- в ходе подготовки к первому этапу ВВУИО (Женева, 10-12 декабря 2003 г.) на национальном и региональном уровнях были проведены первая Бишкекско-Московская конференция по информационному обществу (2002 г.), Международный конгресс в г. Киеве (2003г.), Бакинский международный форум по ИКТ (2003 г.), приняты «Санкт-Петербургская декларация по развитию информационного общества» и «Стратегия сотрудничества стран СНГ в сфере информатизации»;
- в Декларации принципов и Плане действий, принятых на первом этапе ВВУИО, учтена согласованная позиция стран СНГ;
- в целях расширения сотрудничества между регионами на ВВУИО декабря 2003 г. состоялось подписание РСС и региональными союзами (ATU, CEPT, PAPU) «Межрегиональной и международной программы сотрудничества в области связи и информатизации на 2004–2006 гг.»;
- на национальном и региональном уровне осуществляется выполнение решений, предусмотренных итоговыми документами первого этапа ВВУИО, — разрабатываются и реализуются национальные стратегии и программы развития ИКТ;
- в рамках РСС разрабатывается План действий по реализации «Стратегии сотрудничества стран СНГ в сфере информатизации», включающий мероприятия, актуальные для региона.

В то же время на Конференции были отмечены следующие проблемы:

- наличие цифрового разрыва на национальном и региональном уровне, сдерживающего обеспечение доступа населения к услугам ИКТ;

- отсутствие гармонизированной нормативно-правовой базы в сфере ИКТ, что замедляет их внедрение и развитие;
- неадекватность объема финансирования развития ИКТ задачам построения информационного общества в регионе;
- отсутствие ясных механизмов финансирования совместных проектов по развитию ИКТ, а также научно-исследовательских разработок в данной сфере в регионе и недостаточное привлечение донорских средств (международные финансовые институты и организации);
- недостаточный прогресс в сфере обеспечения информационной безопасности и борьбы со спамом;
- отсутствие системы показателей, характеризующих развитие ИКТ и готовность стран к информационному обществу, сопоставимых на региональном и международном уровне, затрудняющее оценку и мониторинг в странах и регионе;
- недостаточность существующей координации построения информационного общества в странах — участницах Конференции между отдельными ведомствами, между государством и частным сектором, а также между странами региона;
- недостаточность механизма обмена информацией со странами других регионов о достижениях в области развития ГИО;
- недостаточная грамотность широких слоев населения для использования возможностей современных ИКТ;
- нехватка высококвалифицированных специалистов в области ИКТ в некоторых странах региона.

На Конференции достигнуто понимание о необходимости:

1. В рамках подготовки ко второму этапу ВВУИО консолидировать усилия участников РСС для продвижения общих согласованных предложений в конкретизирующие документы по реализации решений ВВУИО (в т.ч. по таким ключевым позициям, как вопросы управления Интернетом и создание «Фонда цифровой солидарности»).

2. Одобряя деятельность, осуществляемую в рамках РСС и Координационного совета государств — участников СНГ по информатизации при РСС в части согласования позиции стран — участников РСС по подготовке ко второму этапу ВВУИО, более активно использовать РСС для организации взаимодействия органов госвласти, бизнеса и гражданского общества в построении ГИО.

3. К Московскому этапу Конференции подготовить предложения по созданию механизмов, способствующих развитию сотрудничества, в частности, создание «регионального фонда сотрудничества в сфере ИКТ».

4. Поддержать предложения участников Конференции для включения в План действий РСС и конкретизирующие документы ВВУИО:

- создать механизмы для организации помощи странам с переходной экономикой в формировании информационного общества;
- организовать содействие внедрению международных стандартов в области ИКТ;
- организация подготовки высококвалифицированных специалистов для участия в работе международных организаций связи и ИКТ;
- организация пилотных проектов по цифровому мультимедийному интерактивному вещанию в горных условиях;
- организация региональных координационных программ по важнейшим направлениям развития ИКТ:
- прикладные направления (медицина, образование, государственное управление, охрана окружающей среды и др.);
- развитие законодательства в области ИКТ;
- статистика и мониторинг ИКТ;
- информационная безопасность и борьба со спамом.

5. Обратиться к частному сектору, международным организациям и финансовым институтам осуществлять активное содействие в реализации проектов по развитию ИКТ в регионе СНГ. Конференция призвала все заинтересованные стороны — государство, частный сектор и гражданское общество:

5.1. Объединить свои усилия и активизировать деятельность по выполнению решений, предусмотренных итоговыми документами первого этапа ВВУИО, по следующим основным направлениям в странах региона:

- развитие информационной и телекоммуникационной инфраструктуры и создание общего информационного пространства;
- гармонизация законодательства и нормативно-технической базы;
- разработка и внедрение новых приложений ИКТ (электронное правительство, электронная торговля, электронное здравоохранение, электронное образование и др.);
- либерализация условий торговли услугами ИКТ;
- информационная безопасность.

5.2. При формировании государственных бюджетов стран — участников РСС предусматривать комплексное финансирование «отдель-

ной строкой» развития ИКТ в интересах населения и органов госуправления.

5.3. Осуществлять активное участие в подготовке ко второму этапу ВВУИО, в том числе в работе подготовительного комитета ВВУИО, рабочих групп ООН по управлению Интернетом и определению механизмов финансирования; тематических международных конференциях и форумах.

5.4. Координировать подготовку стран СНГ ко второму этапу ВВУИО в рамках РСС и Координационного совета государств — участников СНГ по информатизации при РСС.

5.5. Подготовить к Московскому этапу Конференции предложения по выработке согласованной позиции и по наиболее приоритетным мероприятиям и проектам для включения в заключительные документы ВВУИО[24].

5.6. Осуществлять в рамках РСС, а также через РСС с другими регионами, постоянный информационный обмен о ходе реализации решений первого этапа ВВУИО, проектов и программ по развитию ИКТ, о планируемых в государствах — участниках РСС форумах по вопросам информационного общества, развитию ИКТ и подготовке ко второму этапу ВВУИО.

5.7. Активизировать проработку странами СНГ вопросов вступления в Координационный совет государств — участников СНГ по информатизации при РСС.

[24] В связи с политическим кризисом в Кыргызстане предложения на август 2005 г. пока не выработаны.

Глава 3
ОТ ЭЛЕКТРОННОЙ КОММЕРЦИИ К ЭЛЕКТРОННОМУ ПРАВИТЕЛЬСТВУ — ЗАРУБЕЖНЫЙ ОПЫТ

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

Дж. ГОЛСУОРСИ

3.1. Основные компоненты электронной коммерции

Исторически первые сделки в рамках электронной коммерции (e-business) возникли в начале 90-х годов. Развившись, они доросли до уровня электронной корпорации (e-corporation). В последнее время появилось немало серьезных исследований, в которых авторы вводят собственные определения виртуальной, или новой экономики и электронной коммерции, а также их компонентов.

Как уже отмечалось в первой главе, глобальная сетевая экономика получила название Networks Economy, а традиционная рыночная экономика называется Economics. Теорию информационно-сетевой экономики некоторые экспер-

ты называют Netnomics[1]. Ее деловая привлекательность и эффективность зависит от наличия в ней экономических агентов и развитой электронной инфраструктуры. Это получило название «Network externalities».

При этом ряд экспертов считают понятие «информационно-сетевая или интернет-экономика» шире понятия «электронный бизнес». Интернет-экономику, которую некоторые аналитики называют и инфономикой, представляет собой глобальную сетевую многоуровневую структуру взаимоотношений между экономическими агентами, осуществляемых через Интернет и другие сети. Она включает в себя индустрию создания новых ИКТ и программных продуктов, телекоммуникационные и провайдерские услуги, электронный бизнес, электронные рынки, электронные биржи, электронные платежные системы, телеработу, дистанционную занятость и другие составляющие. Интернет-экономика развивается в соответствии со своими специфическими целями и критериями эффективности.

Сетевую экономику практически все эксперты рассматривают как единство нескольких составляющих, как по горизонтали, так и по вертикали, а также по уровням. Электронный бизнес, развивающийся на базе высоких технологий, позволяет обеспечить конкурентные преимущества за счет увеличения инвестиций, сокращения затрат, расширения сферы деятельности и выявления новых каналов сбыта, привлечения новых потребителей и улучшения обслуживания клиентов, большей оперативности при принятии управленческих решений.

Электронный бизнес состоит из следующих основных составляющих:

- электронная коммерция (e-commerce);
- электронные закупки (e-procurement);
- электронное обслуживание заказчиков (e-care for customers);
- электронное обслуживание деловых партнеров (e-care for Business Partners);
- электронное обслуживание служащих (e-care for employees);
- электронное обслуживание влиятельных лиц (e-care for influencers).

По мнению большинства экспертов, электронный бизнес включает в себя все возрастающее число компонентов, основными из которых являются следующие[2]:

---

[1] См. Макропропорции Интернет экономики // Технологии информационного общества — Интернет и современное общество: материалы Всероссийской объединенной конференции. СПб., 20-24 ноября 2000 г. — СПб., 2000. С.18-22. http://www.iis.ru/ist2000

[2] Там же.

Предприятие — Предприятие (B2B). B2B имеет место, когда два предприятия осуществляют на основе договоров сделки купли-продажи товаров и услуг, осуществляют платежи, маркетинг через Интернет.

Предприятие — Потребитель (B2C). Продажа предприятием своих товаров и услуг через Интернет потребителям.

Потребитель — Потребитель (C2C). Потребители на основе заключенных сделок с помощью Интернет-провайдеров продают товары другим потребителям.

Потребитель — Предприятие (C2B). Потребители через Интернет делают свой выбор посредством предложения своей цены на различные товары и услуги, предлагаемые предприятиями.

В рамках электронного правительства (подробнее — в следующем параграфе) оказываются следующие электронные услуги: «Правительство — Предприятие» (G2B), а также «Правительство — Потребитель» (G2C). При этом речь идет о предоставлении правительством электронных услуг не просто отдельным потребителям, а покупателям в широком смысле, включая домашние хозяйства. Развивается также такой вид электронного бизнеса, как обмен и продажа через Интернет электронных баз данных (D2G), (D2B) и др.

Вертикальная структура инфономики включает в себя следующие основные уровни:

- Инвестиции и инновации в интернет-индустрии.
- Инфраструктура Интернет.
- Программное обеспечение Интернет.
- Интернет-брокеры, электронный трейдинг и реклама.
- Электронная торговля.
- Оффшорное программирование.
- Индивидуальные услуги в Интернет.

Согласно исследованиям компании IDC, в 2003 г. оборот электронного бизнеса достиг более одного 1,3 триллиона долл., то есть в сто раз превысил оборот 1997 г. Исследования e-Stats показали, что объемы электронной торговли в 2003 г. по типу B2B составили свыше одного триллиона долл., а по типу B2C — свыше 160 млрд долл.[3]

Конвергенция инфономики возникает на основе сетевых интернет-технологий и представляет собой интеграцию или более свобод-

[3] См. *Дятлов С.* Методологическая конвергенция и анализ макропараметров сетевой экономики.

http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/15896a0f9d97f0ebc3256a33003a7637

ное взаимопроникновение различных видов деятельности и переплетение различных функций интернет-компаний при расширении своего бизнеса, при инвестировании, при освоении новой рыночной ниши, что предоставляет им возможность успешно работать на самых различных рынках (товарном рынке, рынке услуг, финансовом рынке). В процессе сетевой конвергенции имеет место определенный интегральный эффект и формируются электронные интегрально интегрированные компании.

Параллельно с формированием различных составляющих сетевой инфономики идет формирование различных сетевых институциональных, управленческих структур, включая институты госвласти на федеральном и региональном уровне. Интернет-технологии не только быстро внедряются в политику, бизнес, госуправление, но и трансформируют характер межличностных отношений в обществе (формируются виртуальные он-лайновые сообщества, устанавливаются отношения информационного партнерства, осуществляется группировка пользователей по определенным информационным интересам), меняют правила «игры», меняют принципы ведения бизнеса, управления компаниями и государственного управления.

В настоящее время между традиционной теорией **Economics** и теорией сетевой экономики **Netnomics** существуют сложные отношения, которые ряд экспертов определяют термином «методологическая конвергенция»[4]. При этом здесь важно учитывать следующие принципиальные особенности.

Во-первых, речь идет о комплексной конвергенции, то есть конвергенции не только предмета и метода исследования, но и методов управления электронно-сетевыми взаимодействиями, инструментария принятия решений и проведения практической политики в сфере инфономики.

Во-вторых, речь идет не просто о конвергенции, понимаемой как механическое сближение методологий рыночной экономики и инфономики, а об эволюционно-конкурентной методологической конвергенции, когда методологии традиционной Economics и Netnomics, взаимообогащаясь и отрицая друг друга, развиваются в одном направлении.

В-третьих, Economics и Netnomics развиваются в направлении, которое характеризуется возникновением и формированием системы принципиально нового коэволюционного типа CINetnomics.

[4] Там же.

Интеграция России в ГИО и глобальную инфономику, обеспечение условий ее перехода на траекторию устойчивого развития требуют выявления целевых стратегий, определения целевых параметров и разработки организационного механизма, учитывающих требования по реализации конкурентных преимуществ российской экономики и обеспечения ее комплексной информационной безопасности. Успешная реализация данных требований предполагает создание системы комплексного мониторинга экономики России и, прежде всего, мониторинга ее наиболее динамично развивающейся подсистемы — электронного бизнеса. Исходной базой для ее создания является определение границ и сферы действия инфономики, исследование ее свойств, функций, выявление уровней, сегментов и элементов ее структуры, что позволит обеспечить построение структурно-функциональной модели инфономики в единстве всех ее составляющих.

Важнейшей задачей разработки такого мониторинга является выявление и выработка системы взаимосвязанных многоуровневых критериев, параметров, показателей и индикаторов инфономики. В рамках системы комплексного мониторинга экономики следует выделять такие его виды, как нано-, микро-, макро- и мегамониторинг. Основной задачей для макромониторинга инфономики является выявление ее системной проблематики на макроуровне, которая представляет собой выявление и анализ сложного комплекса взаимосвязанных проблем, «узких мест», сдерживающих ее динамичное развитие и переход на траекторию устойчивого экономического роста.

В целом в инфономике складываются определенные макропропорции между различными ее составляющими и компонентами. Развитие электронного бизнеса, динамика интернет-экономики может характеризоваться целым набором макропоказателей или макропараметров, которые могут быть классифицированы в соответствии с определенными признаками по самым различным группам.

При этом следует выделить группу показателей, характеризующих объем ВВП, создаваемого в национальном секторе интернет-экономики в течение года (e-GDP). Основной составляющей e-GDP является показатель «общий интернет-доход» (Total Internet Revenues), в который в соответствии с выделяемыми в его структуре сегментами включаются следующие элементы:

1. Доходы интернет-провайдеров за предоставление доступа к интернет-ресурсам.
2. Доходы, получаемые за предоставление интернет-услуг.

3. Доходы от интернет-рекламы.
4. Доходы от интернет-коммерции.

При этом важно учитывать доходы, получаемые экономическими субъектами-инвесторами за счет покупки-продажи акций высокотехнологичных компаний на фондовых рынках.

Традиционные методы регулирования в инфономике перестают быть действенными. Примером этого может служить то, что предпринимаемое правительством в соответствии с неоклассическими постулатами повышение процентной ставки применительно к сфере Инфономики не ведет к снижению потребления населения и не компенсирует «перегрев» экономики и рынка акций высокотехнологичных компаний.

В процессе исследования закономерностей становления и функционирования глобальной инфономики экспертами выделяется следующие недостаточно разработанные макроэкономические проблемы:

- Сетевой информационно-инновационный тип экономического роста и его факторы.
- Формирование новых зависимостей и пропорций между основными секторами и макроэкономическими параметрами в инфономике.
- Конвергенция интернет-бизнеса и новые принципы конкурентной борьбы.
- Налогообложение и таможенные ограничения в электронной торговле.
- Создание новых институциональных органов регулирования инфономики.
- Эмиссия электронных денег и изменение структуры денежных агрегатов.
- Трансформация роли и функций Центрального банка в новой экономике и в регулировании денежной массы, обеспечивающей сделки через Интернет.
- Развитие электронных платежных систем и рост скорости обращения электронных денег.
- Влияние роста количества и скорости обращения электронных денег на инфляцию, на совокупный платежеспособный спрос, на ВНП.
- Влияние инфляции на номинальные и реальные показатели инфономики.
- Возникновение интегральных эффектов.
- Новые критерии оценки стоимости, результативности электронного бизнеса и эффективности инвестиций в проекты электронной коммерции.

- Экспорт программного обеспечения, оффшорное программирование и потери ВВП в результате виртуальной «утечки мозгов».
- Нелинейное ценообразование и модификация функций спроса и предложения на электронные услуги.
- Изменение условий оптимальности и устойчивости краткосрочного и долгосрочного равновесия отдельных рынков и общего макроэкономического равновесия в инфономике и др.

Данные проблемы уже стали предметом научного исследования с целью разработки системы взаимосвязанных макропараметров, показателей и индикаторов инфономики, что должно стать основой для создания системы ее комплексного мониторинга. Рассмотрим лишь некоторые из них.

Первая проблема — это проблема границ национальной экономики и критериев ее отнесения к «открытой» или «закрытой» экономике. Если та или иная страна становится частью глобальной сетевой экономики с развитой информационной инфраструктурой и «прозрачными» электронными границами, то анализ ее макроэкономических параметров функционирования в рамках модели «закрытой экономики» не правомерен. Здесь встает проблема «прозрачности» и открытости границ экономического пространства, что обусловливает модификацию таких инструментов макроэкономического регулирования, как тарифные барьеры и налогообложение. Использование последних в борьбе с экспансией зарубежных корпораций на электронных рынках становится малоэффективным.

В новых условиях появляются новые информационные факторы экономического роста и встает вопрос об **информационно-инновационном типе воспроизводства**. На основе использования интернет-технологий у компаний появляется возможность при сокращении штатов и улучшении менеджмента увеличивать объемы производства и продаж, а также сокращать затраты и увеличивать производительность труда. Это обеспечивает неинфляционный экономический рост, способствует росту эффективности и устойчивости компаний и оказывает благотворное воздействие на будущие ожидания.

В инфономике нарушаются присущие индустриальной рыночной экономике традиционные соответствия, зависимости и пропорции между основными макроэкономическими параметрами и показателями. Например, между экономическим ростом и традиционными факторами, зависимость между динамикой ВВП и инфляцией, между номинальными и реальными макроэкономическими показателями. Также традиционные методы регулирования в инфономике перестают быть действенными. Примером этого может служить то, что

предпринимаемое правительством в соответствии с неоклассическими постулатами повышение процентной ставки применительно к сфере инфономики не ведет к снижению потребления населения и не компенсирует «перегрев» экономики и рынка акций высокотехнологичных компаний.

Развитие электронной торговли выявило целый ряд вопросов, касающихся налогообложения и таможенных ограничений. Применение электронных сделок создает немало трудностей для действующих налоговых органов ввиду анонимности электронной торговли, отсутствия возможности отследить сделки, а также пересечения границ с помощью ИКТ. Организация экономического сотрудничества и развития (ОЭСР), объединяющая 30 наиболее развитых государств мира, разрабатывает рекомендации, в соответствии с которыми налогообложение сделок, осуществляемых в рамках электронной торговли, должно быть нейтральным по сравнению со сделками, осуществляемыми без использования электронных средств. Налогообложение электронной торговли должно соответствовать установившимся международно признанным обычаям и должно осуществляться с наименьшими затратами. Уже имеется определенный опыт в решении этих проблем. Так, ВТО приняла решение освободить от обложения таможенными пошлинами данные и программные продукты, приобретенные и доставленные с помощью Интернет. В США при продажах через Интернет действует мораторий на изъятие налога с продаж, который при обычной торговле составляет 5-10% от цены товара.

Использование современных **электронных платежных систем**, развитие телебанкинга, электронных расчетов приводит к тому, что растет скорость обращения денег. Отсюда возникает ряд проблем: регулирование денежной массы в обращении, влияние массы электронных денег на инфляцию и экономический рост.

Государство в лице Центробанка получает дополнительный доход от эмиссии новых денег («сеньораж»). При появлении электронных денег, встает вопрос о том, кто будет регулировать их массу и получать «сеньораж» и должны ли эмитенты электронных денег быть зарегистрированными, чтобы иметь статус банков. При положительном ответе эмитенты кредитных карточек попали бы под надзор банковских властей. Расхождение во взглядах по данной проблеме отражено в официальных документах ЕС и США.

Актуальная проблема — это интегральные эффекты в результате сетевого взаимодействия в инфономике. Внедрение ИКТ в бизнесе изменило отношение к оценке стоимости бизнеса. Обостряется конкурентная борьба как между традиционными компаниями и интернет-

компаниями, так и среди интернет-компаний. Поглощение их друг другом изменяет сложившиеся пропорции секторов экономики.

В инфономике все труднее отслеживать и учитывать реальные потоки экспорта и импорта, что приводит к неточностям в счетах платежного баланса страны. Последнее приводит к ошибкам при учете доходов и расходов госбюджета и, в конечном счете, к деформации его структуры.

Возникает проблема множественности локальных (в пространстве) или точечных (во времени) балансов и дисбалансов, которые возникают в результате локальных актов купли-продажи и которые практически невозможно отследить. В силу этого резко обостряется проблема регулирования и балансирования локальных сегментов тех или иных рынков.

По мнению экспертов, традиционный принцип определения цены и объема производства путем выравнивания предельного дохода с предельными издержками в инфономике существенно модифицируется, поскольку предельные издержки на производство дополнительной единицы продукции становятся ничтожно малы. В результате спрос и предложение ведут себя особым образом, в частности, повышение спроса не приводит к росту цен. Например, подключение к Интернету все большего числа пользователей не ведет к повышению тарифов, поскольку затраты на их подключение близки к нулю[5].

В этом контексте меняются не только условия оптимальности рынков, но и меняются критерии эффективности инвестиций. Задачи электронной коммерции не соответствуют традиционным критериям, применяемым для принятия решений об инвестировании в проекты, например, показателям, применяемым для возврата инвестиций от вложений в проекты. Здесь возникает ряд новых проблем: сложность расчета показателя отдачи от инвестиций в проекты ИКТ; как измерить степень удовлетворенности клиента; есть ли связь между улучшением удовлетворенности клиента и реальным повышением прибыльности и др.

Дистанционная работа (телетруд). Как уже отмечалось, с развитием ИКТ возникают новые формы занятости, более гибкие распределенные во времени и пространстве графики и режимы работы, которые получили название telecommuting. Эффективность данных видов занятости в виду большей гибкости, оперативности, производительности очевидна и с каждым годом получает все большее и большее распространение.

[5] Там же.

Значительное распространение получил так называемый зарубежный телекомьютинг, когда российские ученые, находясь в России, работают над задачами, присланными им по Интернету от зарубежных компаний. Выполнив их, ученые отправляют их обратно и получают за это зарплату. Данный вид телекомьютинга, усилившийся в последнее время с развитием аутсорсинга, ведет к расширению **виртуальной «утечки мозгов»**.

При этом самоочевидно, что страны-наниматели получают тройной эффект: от экономии на подготовку специалиста, от заниженной оплаты труда этих работников (за счет экономии оплаты жилья, транспорта и др.) и эффект, который приводит к росту ВВП страны-импортера за счет использования интеллектуального труда страны-экспортера. Данный процесс, естественно, приводит к потерям для другой стороны (страны).

Анализ основных трендов развития электронной коммерции показывает ее огромные перспективы и подтверждает ранее выдвинутый тезис (см. 2.3.4.) о том, что Интернет, как основа инфономики, нуждается в скорейшем международно-правовом регулировании.

3.2. Модели электронного правительства

В середине 90-х годов пришло понимание, что **не существует принципиальной разницы между процессами автоматизации в большой корпорации и в государстве**, что можно использовать существующие наработки и методики для повышения эффективности госуправления. К тому же в это время правительства многих стран столкнулись с необходимостью пересмотра классических моделей госуправления, которые оказались неадекватными новым условиям. Тогда и появилось понятие «электронное правительство» (ЭП). Тогда же сформировались и родственные ему понятия, такие как «электронная демократия» (e-democracy), «электронное управление» (e-governance). В настоящее время, когда во многих странах уже функционируют основные составляющие ЭП, можно констатировать, что **суть ЭП — это внедрение корпоративной информационной системы национального масштаба**.

В развитых странах и в большинстве развивающихся стран разработаны и реализуются стратегии или комплексные программы информационного развития как общества в целом, так и отдельных сфер деятельности.

Анализ таких стратегий и программ в странах Евросоюза, Балтийского региона Европы, Японии, США, Индии, Бразилии, Мексики показывает, что их основной целью является достижение лидирующих

позиций в экономике и в социальном развитии. Отличительная их особенность состоит в том, что они рассматривают все используемые сетевые технологии — электронную коммерцию, электронное правительство, электронный бизнес и т. д., не как изолированные сферы деятельности, а как интегрированную и взаимозависимую совокупность этих технологий, которые составляют единый фундамент перехода к информационному обществу.

Во всех стратегиях отмечается ведущая роль государства в формировании национальной стратегии информационного развития, в консолидации всех слоев общества в формировании партнерских отношений между всеми участниками информационного развития и координации совместной деятельности государства, бизнеса, всех общественных институтов и граждан в его реализации для решения сформулированных целей информационного развития.

Опыт стран, уже вступивших на путь постиндустриального развития, показывает, что в этих странах опережающими темпами происходит развитие экономики, основанной на использовании не только непосредственно интеллектуальных и информационных ресурсов, но и на использовании качественно новых свойств информационной среды для рационального использования таких традиционных ресурсов, как природные, человеческие, финансовые.

Вместе с тем мировой опыт показывает (и это уже выше отмечалось), что информационное развитие порождает целый комплекс негативных геополитических последствий. Прежде всего, это ускорение поляризации мира, увеличение разрыва между богатыми и бедными, технологически передовыми и отсталыми странами, что является главным источником нестабильности, сегодняшних и будущих конфликтов, в том числе глобального характера.

Государство является одним из главных фигурантов формирования информационного общества. Одновременно, **с развитием инфообщества, само государство не может продолжать работать по-старому**. В силу этого уже около 10 лет в развитых странах создаются отвечающие своим национальным интересам электронные правительства.

Проблематика электронного правительства — калька с английского «e-Government» — прочно вошла в политический лексикон, в том числе в ООН, ОЭСР, Евросоюзе и в других важных международных структурах в конце XX века. Вместе с тем, по мнению ряда известных исследователей, подход к данной про-

блеме на начальном этапе страдал отсутствием системности и концептуальной гармоничности[6]. При анализе ЭП чаще рассматривались применяемые вэб-технологии, электронный документооборот, финансовые аспекты, приводились примеры и модели его успешного внедрения. При этом в целом **преобладал эйфорийный подход, а ЭП выдавалось чуть ли не как панацея от большинства накопившихся проблем социума и его отношений с государством.**

Следует отметить, что в последнее время появились действительно системные работы по теме ЭП и связанным с ним социальным и иным проблемам, в т.ч. по таким, как развитие гражданского общества и демократии. Весомый вклад в этот процесс внесла подготовка и проведение ВВУИО в Женеве, а также реализация принятых декларации и плана действий, в т.ч. в ходе подготовки к Тунисскому этапу ВВУИО (см. 2.3.5.).

Итак, ЭП призвано выполнять функции регулирования информационных отношений между основными субъектами и государственными структурами. Среди целого ряда задач, решаемых ЭП, следует выделить следующие важнейшие его составляющие:

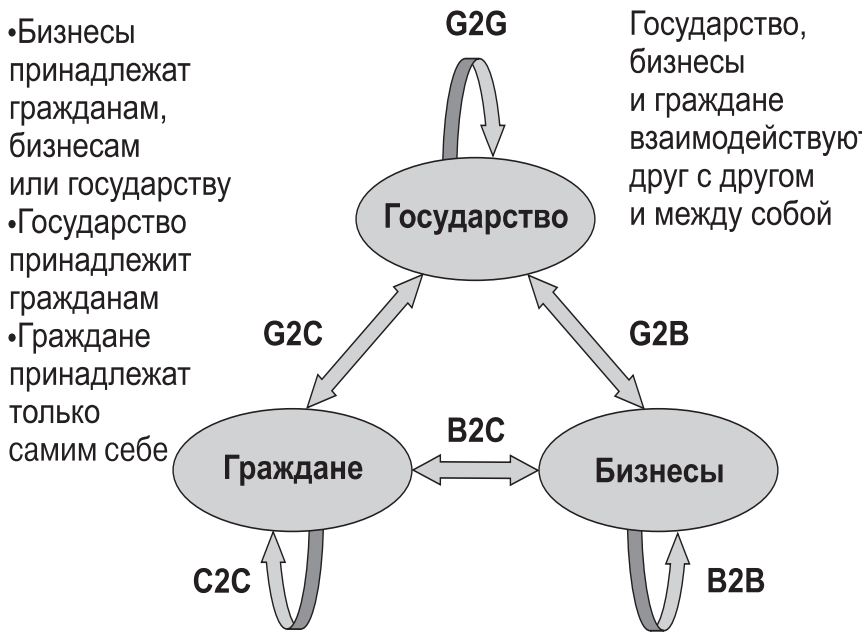
- как обеспечение равных прав и доступа к глобальным, национальным, местным и локальным информационным ресурсам;
- предоставление необходимой информации и электронных услуг гражданам;
- осуществление электронных государственных закупок;
- содействие развитию инфономики;
- регулирование взаимоотношений между основными субъектами электронного бизнеса;
- осуществление дистанционных фискальных и контрольных функций;
- оказание дистанционных консультаций;
- обеспечение информационной безопасности и др.

Несмотря на динамичное развитие современных стран, их политическую систему достаточно упрощенно можно представить как совокупность взаимодействия трех субъектов — государства, граждан и бизнеса. Взаимодействие между ними выражается B2B (business-to-business), B2C (business-to-customer), G2B (government-to-business), G2C (government-to-citizen) и т.д., которое можно отобразить по следующей схеме[7].

---

[6] См. *Агамирзян И.Р.* Информационное общество. 2002. Вып. 1. С. 56-62.

[7] Там же.



Под электронным правительством понимается система государственного управления на основе электронных средств обработки, передачи и распространения информации.

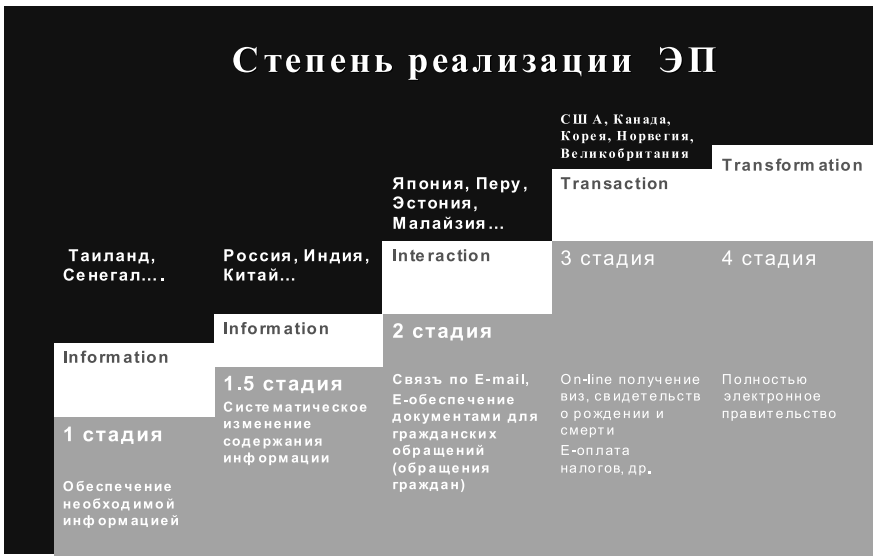
Среди огромного количества определений ЭП чаще используется следующее — это организация госуправления и местного самоуправления на основе электронных средств обработки, передачи и распространения информации, предоставления общественных услуг всем категориям граждан (пенсионерам, рабочим, бизнесменам, госслужащим и др.) электронными средствами.

Основными целями ЭП являются:

- Достижение максимальной доступности услуг госорганов и органов МСУ для населения и бизнеса.
- Осведомленность, прозрачность и борьба с коррупцией.
- Наибольшая эффективность работы госорганов и органов МСУ
- Улучшение бизнес-климата для иностранных инвестиций.

- Обеспечение информбезопасности личности, общества и государства.
- Создание системы свободного и равноправного получения, распространения и использования информации.

По степени реализации ЭП страны можно достаточно условно разделить (в т.ч. и на основе оценок МСЭ — см. 2.1.2.) на следующие пять групп.



Основные стадии внедрения электронного правительства:

1. **Начальная** — связана с выходом правительственных структур в электронные сетевые структуры. На этом этапе правительства имеют один или несколько сайтов, которые выполняют информационную роль.

1.5. **Расширенное интернет-присутствие** — позволяет пользователям получать специализированную и постоянно обновляемую информацию через правительственные сайты. При этом обеспечивается получение правительственных публикаций, правовых документов, новостной информации. Появляется информация об электронных адресах, внедряются поисковые системы, у посетителя вэб-сайта возникает возможность передать сообщение — вопрос или комментарий — по электронной почте.

2. **Интерактивное взаимодействие** — характеризуется интенсификацией взаимодействия между гражданами (бизнесами) и правительственными структурами. Возникают правительственные вэб-порталы, позволяющие пользователям напрямую иметь доступ к информации, соответствующей их конкретным потребностям и интересам. Пользователь может получать специализированные данные, загружать различные формы и бланки, используя механизмы аутентификации.

3. **Проведение транзакций** — включает возможности для пользователя получать через сеть документы и осуществлять сделки. Граждане могут получать визы, паспорта, свидетельства о рождении и смерти, лицензии, разрешения и другие трансакционные услуги. Правительственный вэб-портал обеспечивает прямой доступ граждан к правительственным подразделениям и услугам. Граждане могут платить налоги и осуществлять другие платежи через Сеть, используя для этого электронную подпись.

4. **«Бесшовное взаимодействие»** — полностью интегрированное вэб-присутствие — отличается тем, что позволяет правительству осуществлять все услуги, а пользователю — получать любую услугу через правительственный портал.

Из-за неравномерности экономического развития стран мира внедрение ЭП в них находится на разных стадиях. Например, если сегодня в развитых странах происходит переход к поколению транзакций, Government Gateways — «шлюзы одного окна», то в большинстве стран мира ЭП пока не выходит за рамки интерактивного вэб-присутствия (правительственных порталов).

Широкое понимание ЭП определяет не только новый характер отношений, но и трансформацию всего комплекса отношений госуправления с обществом. Вместе с тем очевидна и бессмысленность автоматизации существующих неэффективных процедур управления. Если провести аналогию между корпорацией и государством, то можно сослаться на известный факт, заключающийся в том, что повышение эффективности функционирования корпорации в целом при внедрении ИКТ достигается только при одновременном проведении реинжиниринга основных бизнес-процессов.

В течение десятилетия развития концепции ЭП выработаны и устоялись основные принципы его организации:

- открытость;
- «принцип одного окна»;
- обратная связь.

Реализованный во многих странах «принцип одного окна» во взаимоотношениях бизнеса с клиентами в ЭП необходимо распростра-

нять на взаимоотношения государства и граждан, государства и бизнеса. Весь взаимообмен документами и обмен информацией должен происходить внутри государственных учреждений, без участия гражданина. Реализация обратной связи исполнительной власти с населением в концепции электронного правительства приобретает особое значение в плане демократизации госвласти, «электронной демократии». Обратная связь — это основной принцип мониторинга реакции на деятельность органов исполнительной власти. Она может быть использована государством для корректировки отклонений от планируемых процессов.

Во многих странах разрабатываются национальные программы перехода к информационному обществу, которые включают проекты создания и развития ЭП. В качестве примеров можно привести национальные программы Великобритании UK online, США «Национальная информационная инфраструктура», Франции Government Action Program for Information Society, России «Электронная Россия», общеевропейскую программу eEurope, программу стран «Группы семи» «Государство он-лайн».

Согласно директиве eEurope 2002 Action Plan, принятой ЕС в июне 2000 г., в 2005 г. в европейских странах должна быть реализована программа создания национальных электронных правительств (подробнее — в 3.4.1). Под этим подразумевается в первую очередь предоставление гражданам информации и услуг госорганов всех уровней посредством Интернета. И уже на первом этапе в ряде более развитых стран перевод деятельности госаппарата в электронную форму стал реальностью. В ближайшие годы правительства и госорганы европейских стран планируют перевод своих служб на онлайновые режимы. Например, правительство Франции в 2001 г. объявило о намерении в 2005 г. реализовать первую в мире систему A2C (administration-to-consumer), в рамках которой предполагается все административные услуги гражданам предоставлять через Интернет.

Ниша проектов по созданию ЭП сегодня заполняется крупнейшими мировыми производителями решений — Microsoft, SAP, Oracle и пр. Как правило, генеральным подрядчиком выступает крупная и хорошо известная консалтинговая фирма. Так, компании Arthur Andersen и Microsoft сформировали альянс по работе с госорганами Эстонии, Латвии и Литвы. В Болгарии же, например, создан совет из местных представительств международных компаний Hewlett-Packard, IBM, Microsoft и Cisco Systems. В ответ болгарская ассоциация местных компаний (BAIT), работающих в области ИКТ, выразила свое

неудовольствие, считая, что их интересы тоже надо учитывать при дележе заказов.

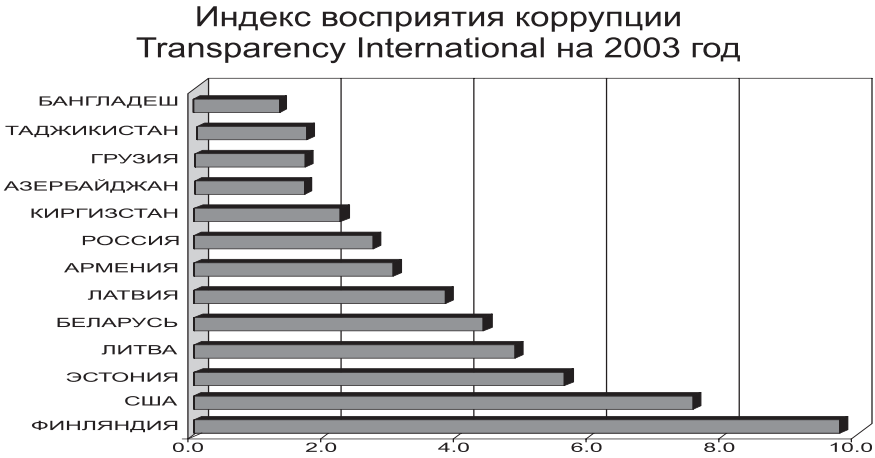
В **Канаде** разработан ряд программ по интенсификации использования информационных технологий под общим названием «Общающиеся канадцы» (Connecting Canadians). Уже сейчас здесь действуют три правительственных портала, обеспечивающие коммуникацию и взаимодействие между гражданами и правительством. Это «Канадский сайт» (Canada Site, canada.gs.ca), «Правительство онлайн» (Government On-Line, www.gol-ged.gs.ca) и «На службе Канады» (Service Canada, www.servisecanada.gs.ca).

3.2.1. ЭП как способ борьбы с коррупцией

По данным информационно-аналитического агентства «Тренд»[8] коррупция стала неотъемлемой частью экономики и политики многих стран. МВФ считает, что 8% мировой экономики работает за счет незаконно полученных средств. Взятка становится важным пунктом почти в любой сделке, достигая в иных странах 20% контракта. По данным ОЭСР, потери мировой экономики от коррупции составляют от 500 млрд до 1 трлн долларов в год. Особенно бурно коррупция развивается в странах с переходной экономикой, в том числе и в республиках бывшего СССР. По результатам исследования, проведенного Всемирным банком в 2002 г. в 97 странах, Украина, Россия, Азербайджан, Казахстан и Узбекистан получили максимальный балл коррумпированности. Международная организация Transparency International (TI) 7 октября 2003 г. опубликовала ежегодный отчет «Индекс восприятия коррупции», в котором рассмотрено положение с коррупцией в 133 странах мира. Индекс восприятия коррупции (ИВК), составляемый TI, ранжирует эти страны в зависимости от степени представлений о распространенности коррупции среди госслужащих и политиков. Это составной индекс, основанный на данных 17 различных опросов и исследований, проведенных 13 независимыми организациями среди предпринимателей и местных аналитиков, включая опросы жителей данной страны — как ее граждан, так и иностранцев. Для исследования брались как минимум три отчета от каждой страны.

---

[8] http://www.pfmc.az/cgi-bin/cl2_fmc/item.cgi?lang=ru&item=20040621134837339 N 49(159). 15 декабря 2003 г.



Наименее коррумпированной страной в мире является Финляндия, за которой следуют Исландия, Дания и Новая Зеландия. Германия — на 16-м месте, Франция — на 23-м, Греция — на 50-м. Из стран СНГ Белоруссия — на 53-м месте, у Армении 78-е место и России 87-е место. Из республик СНГ самое катастрофическое положение с коррупцией в Азербайджане, Грузии и Таджикистане, которые заняли соответственно 125-е, 127-е и 128-е места. Самые коррумпированные страны в мире — Нигерия и Бангладеш. Основным источником коррупции эксперты считают вмешательство государства в экономику.

С учетом того, что суть ЭП заключается в переносе деятельности правительства в Интернет, резко увеличивается прозрачность и эффективность работы. Это достигается, как известно, во-первых, за счет прохождения процессов передачи информации и финансовых потоков фактически в режиме реального времени; во-вторых, за счет снижения затрат; в-третьих, за счет увеличения качества предоставляемых услуг; в-четвертых, с увеличением прозрачности отношений государства и граждан. При этом фактически весь процесс происходит без прямого участия чиновников.

Основная идея развития ЭП на Западе — это использование ИКТ для увеличения степени открытости и подотчетности деятельности правительств обычным гражданам. Три примера, представленных Всемирным банком (из Южной Кореи, Аргентины и Индии), наглядно демонстрируют, что повышение степени открытости информации о решениях и действиях чиновников, а также повышение роли общественного участия значительно снизили уровень коррупции среди госслужащих.

Вышесказанное убедительно показывает, что ЭП — это не только важный шаг, являющийся ключевым звеном в модернизации правительства, но и одно из перспективных направлений борьбы с коррупцией на госуровне.

3.3. «E-government» США

Несомненное лидерство США в области формирования национального информационного общества обусловлено тем, что федеральные власти отчетливо осознают доминирующую роль ИКТ в развитии своей экономики и повышении ее конкурентоспособности на мировом рынке. Американское правительство ведет целенаправленную политику поддержки науки, высоких технологий вообще и ИКТ в частности.

В 1993 г. правительство США выпустило доклад с планами развития национальной информационной инфраструктуры (НИИ) (Agenda for Action). Для изучения проблем связанных с построением НИИ, была создана Рабочая группа по информационной инфраструктуре (Information Infrastructure Task Force).

Было предложено 9 руководящих принципов:

- поощрение частных инвестиций;
- концепция универсального доступа;
- помощь в технологических инновациях;
- обеспечение интерактивного доступа;
- защита личной жизни, безопасности и надежности сетей;
- улучшенное управление спектром радиочастот;
- защита прав интеллектуальной собственности;
- координация государственных усилий;
- обеспечение доступа к государственной информации.

(Information Superhighway: An Overview of Technology Challenges, Report to the USA Congress, 1995).

Правительство США сделало развитие НИИ и глобальной информационной инфраструктуры (ГИИ) приоритетами своей политики.

Работы по созданию собственно ЭП в США начались в 1997 г. в рамках программы национального партнерства по усовершенствованию правительственной структуры. Для разработки научных основ и долгосрочной стратегии развития информационной политики Национальная академия наук США объявила программу грандов по данной теме, призванную стимулировать фундаментальные и приклад-

ные исследования в области применения новых ИКТ в деятельности правительственных учреждений на всех уровнях власти. Задачей программы является создание новых методов администрирования, в т.ч. и основанных на современных ИКТ, которые позволили бы сократить расходы на содержание правительственного аппарата, увеличить эффективность и транспарентность его функционирования.

Анализ общих принципов стратегии правительства США в области ИКТ позволяет утверждать, что правительство:

- заинтересовано в обеспечении больших удобств для граждан во взаимоотношениях с госучреждениями;
- принимает на себя роль лидера в электронизации экономики, в том числе в стимулировании развития е-коммерции;
- реорганизует свою работу в рамках национальной инициативы по усилению контроля за своей деятельностью со стороны граждан.

Особое внимание федеральное правительство США уделяет:

- электронной торговле между госорганизациями и министерствами, конкурсным е-торгам на поставки товаров и услуг для удовлетворения госнужд;
- доступу населения к правительственной и административной информации;
- использованию смарт-карт, в том числе в федеральном правительстве[9];
- решению различного рода задач, в частности получению официальных документов через правительственные Web-сайты, оплате налогов, предоставлению информации о работе госаппарата населению и др.;
- применению ИКТ в медицине и здравоохранении.

Доступность федерального руководства и президента США для населения страны обеспечена системой Comlink[10], разработанной в Массачусетском технологическом институте. Система имеет совершенные службы и средства публикации правительственных документов и открыта для доступа пользователям Интернета. Предоставляемые канцелярией Белого дома материалы брифингов, речи, отчеты, проекты законов и т. д. размещаются на сервере распространения электронной информации системы Comlink, и, по оценкам специалистов, более миллиона пользователей ежедневно получают интересующие их документы.

---

[9] http://smart.gov

[10] www.ai.mit.edu/projects/iiip/doc/comlink/ overview.html

Другая система — Open Meeting[11] — была реализована в рамках уже упомянутой выше инициативы National Performance Review (NPR). Она позволяет подавать предложения и получать отклики на них в интерактивном режиме по электронной почте. Одной из главных целей создания системы было упрощение проведения опросов и получения комментариев из множества разнообразных источников.

Обе системы позволили сделать правительство доступным для населения страны и обеспечить граждан совершенными средствами доступа к государственным документам и выбранным представителям в органах управления. В то же время федеральные служащие получили возможность отслеживать настроения избирателей.

Значительным шагом в данном направлении стало создание национального электронного мегапортала, объединяющего целую сеть интернет-сайтов и предоставляющего унифицированный доступ к сетевым ресурсам большинства законодательных, исполнительных и судебных структур государства.

Американский путь формирования ЭП определяется общей моделью социально-экономического развития, в которой функции государства сводятся к минимуму, а деятельность частных лиц — к максимуму. Главное в этом подходе — оставить все в руках частного сектора и сил рынка, полная либерализация рынка ИКТ.

В США, где электронные технологии в правительственной деятельности связаны еще с административными реформами начала 90-х годов, движение за ЭП интенсифицировались с приходом новой администрации Джорджа Буша-младшего. Это движение положено в основу административной реформы нового столетия. Руководство США опубликовало стратегический документ по электронному правительству, в котором говорится:

1. Правительство должно концентрироваться на гражданах, а не на бюрократии.

2. Правительство должно ориентироваться на результаты своей деятельности.

3. Правительство должно базироваться на рынке, активно продвигая инновации.

Федеральное правительство США на реализацию программы ЭП выделяет несколько миллиардов долларов. Главный правительственный портал США First Gov[12], введенный в действие в 2000 г., служит реализации основных целей пятого этапа внедрения ИКТ в госуправ-

[11] www.ai.mit.edu/projects/iiip/doc/open-meeting/ abstract.html

[12] www.firstgov.gov

ление. Он построен в соответствии с основной концепцией ЭП как системы отношений правительство — граждане, правительство — бизнес, межагентских отношений. Этот портал объединил свыше 27 млн федеральных правительственных страниц с целью более эффективного поиска информации и оказания услуг, следуя потребностям пользователей. Важнейшей функцией электронного правительства является сбор налогов и штрафов через Интернет. Предполагается, что в 2006 г. все уровни правительства в США будут собирать через Интернет 15 % всех налогов и штрафов, что составит $602 млрд. Вместе с тем администрация США к началу 2003 г. заняла лишь третье место в мире по качеству общения с гражданами с помощью Интернета. На первом месте оказалась Канада, а на втором — Сингапур. Этот вывод был сделан исследовательской фирмой Accenture. При составлении рейтинга Accenture учитывала ряд факторов, в том числе количество правительственных сайтов, качество предоставляемых ими услуг, долю жителей страны, постоянно пользующихся ими.

3.3.1. Нормативно-правовая база

Принципиально важно, что ЭП США обеспечено необходимыми нормативно-правовыми документами. Наиболее важные из них следующие:

1. Закон о свободе информации США 1996 г. (Freedom of Information Act.).
2. Закон Клингера Коэна США 1996 г. Clinger-Cohen Act of 1996 (Public Law No: 104-208), Закон о реформе управления ИКТ. Этот акт обязывает все государственные агентства фокусироваться на результатах, которые они достигают, инвестируя в ИКТ.

3. Законодательный акт S-803 от 15 июня 2001 г. «Об электронном правительстве США» (US E-Government Act of 2001). Акт предусматривал:

— создание в составе Административно-бюджетного департамента (US Office of Management and Budget, OMB) Отдела информационной политики (Office of Information Policy) во главе с федеральным директором по информационным технологиям (Federal CIO), статус которого предусматривает верховное администрирование и контроль деятельности органов и должностных лиц исполнительной власти в сфере определения и воплощения государственной информационной политики, а также генеральное руководство и координацию разработки и выполнения федеральных проектов и программ электронного правительства;

— организацию общенационального Совета директоров по информационным технологиям (CIO Council), предназначенного для совместной работы с федеральным CIO в области разработки, реализации и развития совместных межведомственных информационно-технологических инициатив правительства США, надзора за совершенствованием и соблюдением законодательно-правовой и нормативно-технической базы государственной информационно-технической политики, а также для сотрудничества с Департаментом управления кадрами правительства США (Office of Personnel and Management, OPM) по вопросам обеспечения правительственных учреждений квалифицированными специалистами, ориентированными на выполнение этими учреждениями возложенных на них ИКТ функций;

— в целях финансового обеспечения межведомственных информационно-технологических проектов и программ образование государственного Фонда развития ЭП (E-Government Fund), объем которого из бюджетных и иных поступлений был определен в размере 200 млн долл. в год и управление которым поручено Федеральному CIO;

— учреждение при Отделе информационной политики Федерального информационно-технологического учебного центра (Federal Information Technology Training Center), задачей которого является специальная подготовка и обучение персонала правительственных учреждений применению информационно-технических средств и пользованию информационными ресурсами;

— основание Национальной онлайновой библиотеки (Online National Library), формирование и обеспечение работы которой под руководством федерального CIO поручено консорциуму государственных информационных учреждений в составе Национального научного фонда, Смитсонианского института, Института музейных и библиотечных наук и Библиотеки Конгресса США.

4. Изменения и дополнения от 27 июня 2002 г. к Законодательному акту S-803 «Об электронном правительстве США» (US E-Government Act of 2002):

— в составе Административно-бюджетного департамента создан Отдел электронного правительства (Office of Electronic Government) во главе с администратором, статус которого предусматривает верховное администрирование и контроль деятельности органов и должностных лиц исполнительной власти в рамках политики и стратегии электронного государственного управления, а также генеральное руководство и координацию разработки и выполнения федеральных проектов и программ электронного правительства;

— организован общенациональный Совет директоров по информационным технологиям, уполномоченный и предназначенный для совместной работы с заместителем директора Административно-бюджетного департамента по управлению и администратором Отдела ЭП в области разработки, реализации и развития совместных межведомственных информационно-технологических инициатив правительства США, а также для сотрудничества с Департаментом управления кадрами правительства США по вопросам обеспечения правительственных учреждений квалифицированными специалистами, ориентированными на выполнение этими учреждениями возложенных на них информационно-технологических функций;

— управление государственным Фондом развития электронного правительства поручено администратору Департамента общих служб США (General Services Administration, GSA)[13].

3.3.2. Основные функции ЭП США

Основные функции ЭП США включают в себя организацию доступа граждан к электронным базам данных правительства и администраций штатов, предоставление форм и бланков документов через Web-сайты, а также использование их для оплаты налогов, регистрацию транспортных средств и патентов. Одним из важных элементов является обеспечение контроля за прохождением запросов и документов, направляемых в госструктуры, что позволяет в любой момент определить их текущий статус. Большое внимание уделяется организации электронной торговли между госорганизациями и частным сектором и конкурсным электронным торгам на поставки товаров и услуг для нужд государства, в т.ч. и для военных ведомств.

Стратегия развития e-government в США нацелена на повышение эффективности работы федерального правительства следующими способами[14]:

- упрощение информационного сервиса;
- исключение дублирующих друг друга и избыточных уровней правительственного управления; облегчение поиска информации и получения услуг от федерального правительства для граждан, предпринимателей, правительственных и федеральных служащих;
- нацеленность правительственных структур на быстрое удовлетворение потребностей граждан;

[13] http://www.cio-world.ru/offline/2004/31/36990/

[14] http://conf.infosoc.ru/2003/03-rGOVf07.html

- создание условий для претворения в жизнь других инициатив федерального правительства по повышению эффективности его деятельности.

Согласно разработанной стратегии, одной из главных целей развития e-government является сокращение масштабов, а в идеале и полное искоренение дублирования одних и тех же функций в разных правительственных структурах для того, чтобы облегчить гражданам доступ к ним и сократить расходы на содержание избыточных служб и ведомств.

Доступ населения к информации о деятельности правительства и президента обеспечивается через сайты госучреждений в Интернете, а также системой Comlink[15]. По статистике к этим сайтам ежедневно обращается свыше десяти миллионов пользователей сети Интернет. Предусматривается обратная связь, которая предполагает получение комментариев из широкого спектра источников. Обсуждаемый материал структурируется по разделам, и каждый участник обсуждения может выбрать интересующую его тему.

Правительство США и власти штатов предложили населению сотни интерактивных услуг. Они включают в себя оплату налогов, штрафов, продление лицензий на различные виды предпринимательской деятельности и многое другое. Так, согласно проведенному в штате Аризона исследованию интерактивное продление лицензии в среднем обходится гражданам в 2 долл. Осуществление той же операции через кассу госучреждения обходится в среднем в 7 долл. Учитывая, что только в этом штате ежегодно предоставляется 800 тыс. лицензий, экономия только на этой услуге превышает 4 млн. долл.

Реформы, связанные с созданием ЭП, коснулись министерства торговли США. На его сайтах, к числу услуг которых относятся подача заявок на экспортные лицензии и товарные знаки, поиск патентов, ежедневно регистрируется порядка 2,5 млн обращений. Большая часть данных патентной службы США, относящейся к этому министерству, уже доступна в режиме он-лайн, в т.ч патенты, хранящиеся в архивах с XVIII в.

Создание электронных механизмов осуществления работы правительства затрагивает также и сферу международной торговли. Администрация проводит переговоры с рядом государств по созданию унифицированной системы обмена открытых ключей для верификации электронных цифровых подписей контрактов, что значительно упростит осуществление электронной коммерции за пределами страны.

[15] http://www.firstgov.gov/

Агентство по чрезвычайным ситуациям также создало централизованную систему, объединяющую непосредственно или через промежуточные звенья персональные компьютеры, цифровое телевидение, средства беспроводного доступа, телефоны и иные приборы с операторами центров экстренного вызова.

Отличительной особенностью перестройки деятельности правительства США является тесное взаимодействие с деловыми кругами. Представители частного сектора обеспечивают необходимую инфраструктуру и обслуживание систем ЭП США. О своих проектах объявили такие компании, как IBM, Ariba и Commerce One. Две последние компании осуществляют продажу правительству соответствующих программных продуктов через своих дистрибьюторов Govplace.com и iGov.com.

Кроме того, существует множество более мелких компаний, которые предлагают госорганам различные системные решения. Например, Digital Commerce Corporation (DCC) поддерживает целую серию Интернет-сайтов для правительства. Так, сайт StateGovCenter.com[16] — предстаавляет электронный рынок, на котором власти штатов и местные органы власти закупают необходимую продукцию. Безусловным лидером в данной области является компания National Information Consortium (NIC).

В апреле 2003 г. администрация Джорджа Буша создала интернет-сервис, воспользовавшись которым, любой пользователь Сети может задавать вопросы напрямую чиновникам аппарата президента США. Общение происходит в режиме реального времени, так что у посетителей сайта «Спроси у Белого дома» (Ask the White House) есть шанс получить ответ немедленно. При этом ответа на свой вопрос можно и не получить, так как интервьюируемый чиновник сам выбирает, на какие вопросы отвечать.

3.3.3. Роль главных специалистов по ЭП (CIO)

По мере развития процессов информатизации госуправления в отдельных странах, по мере активизации глобального сотрудничества в этой области все чаще поднимаются и дебатируются в различных инстанциях вопросы, связанные со статусом, компетенцией, полномочиями и функциями «первого информационно-технологического лица». Должность главного правительственного специалиста по информационным технологиям, государственного ИТ-начальника или,

[16] http://www.StateGovCenter.com

иначе говоря, CIO национального масштаба, до сих пор весьма неоднозначна во всех отношениях.

Одним из последних примеров подобной дискуссии стал организованный Всемирным банком в конце сентября 2004 г. международный видеосеминар «Руководство строительством электронных правительств: проблемы становления фигуры CIO в государственном секторе»[17]. В его пресс-релизе отмечалось, что семинар представляет собой ответ Всемирного банка на растущий во многих странах мира интерес к повышению роли лидеров в управлении информатизацией своих государственных ведомств, внутри- и межведомственной координации работ в области ИКТ и возможностям исполнения этой роли должностными лицами в ранге CIO на национальном, региональном и ведомственном уровнях.

Начиная с 1998 года аналитики и эксперты, корреспонденты и обозреватели и высокопоставленные официальные лица США, имеющие хоть какое-то отношение к информатизации административных функций государства, стали пропагандировать идею создания института федеральных CIO, аналогичного в американском бизнесе, без которого, как писал в то время журнал «InformationWeek», здание ЭП может или остаться без фундамента, или перекоситься по ходу стройки, или развалиться на несколько изолированных строений, лишенных электричества, теплоснабжения и иных коммуникаций.

В течение президентской кампании 2000 г. оба кандидата, Альберт Гор и Джордж Буш, вместе с окружавшими их уважаемыми парламентариями и ИКТ-профессионалами, каждый по-своему акцентировали внимание общественности на необходимости учреждения должности главного CIO государства и наделения его значительными средствами и полномочиями. Однако уже с момента своего возникновения эти инициативы стали наталкиваться на жесткое сопротивление целого ряда правительственных органов — и прежде всего силовых структур, которые увидели в формировании централизованного ИКТ-руководства попытку вторжения в их закрытую от посторонних глаз информационную епархию.

После избрания Буша президентом проблематика правительственного руководства ИКТ на некоторое время отошла на второй план. Однако, когда вопрос о федеральном CIO вновь начинал дискутироваться, официальные лица, подтверждая приверженность курса новой администрации на создание эффективного аппарата

[17] http://www.cio-world.ru/offline/2004/31/36990/

на базе ИКТ-управления, говорили о подготовке законопроекта, в соответствии с которым функции федерального CIO будут поручены первому заместителю председателя влиятельнейшего Административно-бюджетного департамента (US Office of Management and Budget, OMB). Но по мере того, как этот законопроект проходил согласующие инстанции и приобретал окончательные очертания, тональность подобных заявлений заметно менялась. Уже в начале 2001 г. пресс-секретарь Белого дома Ари Флейшнер выступил с заявлением о том, что в процессе формирования структуры главного CIO страны его функции рассматривались не как организационно-распорядительные, а прежде всего как координационные.

В законопроект (получивший неофициальное название «E-Government Act — 2001») прошел процедуру парламентского утверждения в мае 2001 г., но еще двумя месяцами ранее, комментируя его содержание, зампредседателя OMB Шон О'Кифи заметил, что федеральным CIO станет вовсе не он лично, а делегируемый на эту должность Марк Форман, сфера деятельности которого будет распространяться на администрирование, контроль и координацию работ исполнительных органов в области реализации проектов и программ ЭП, и для этих целей в распоряжение CIO № 1 поступает вновь создаваемый в составе OMB Отдел информационной политики и специальный Фонд развития электронного правительства, учреждаемый в размере 200 млн долларов в год.

«E-Government Act — 2001» вступил в силу, но на этом процесс обсуждения задач и функций главного CIO не закончился. В течение нескольких месяцев по инициативе конгрессменов Тернера и Дэвиса была развернута кампания по внесению изменений в только что принятый закон, проходившая под лозунгами о том, что федеральный chief information officer в конечном итоге подомнет под себя всех своих ведомственных коллег, узурпирует их полномочия и внесет сумятицу в уже налаженную систему ИКТ-управления министерствами, департаментами и прочими госинститутами. Стремление к сохранению организационно-технологической независимости министерств и ведомств и превращению новорожденного федерального CIO в очередного кабинетного чиновника было очевидным, но настолько энергичным, что предложения Тернера и Дэвиса в конце концов были приняты и год спустя в виде откорректированного закона «E-Government Act — 2002» стали окончательной правовой основой деятельности верховного ИКТ-директора США со всеми его урезанными функциями.

3.3.4. Интегрированная информационная система Госдепартамента США

Наиболее амбициозная ведомственная программа развития информационной системы создается в Госдепартаменте США, которая, по сути, поставлена в центр всех информсистем госорганов. Из материалов Госдепартамента США, доложенных Комитету Палаты представителей по правительственной реформе 26 февраля 2002 г., заслуживает внимания следующее:

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

- передача по электронной почте конфиденциальной и секретной информации;
- программа безопасного голосового и прямого соединения с публичной федеральной сетью, а также с сетями Минобороны и Госдепа;
- программа радиоподдержки в чрезвычайных ситуациях;
- почтовые и телеграфные услуги, в т.ч. для личной переписки;
- телекоммуникационные и компьютерные услуги (спутниковая связь, провайдеры Интернета, радиосети местной защиты и т.д.);
- телекоммуникационные сети для получения дипломатических сообщений с криптографической защитой и мониторингом безопасности каналов связи.

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

- к середине 2004 г. внедрить новую интегрированную систему передачи сообщений (сбор, обработка, использование, распределение, архивирование и поиск всех государственных сообщений, включая внутренние меморандумы, электронную почту, официальные сообщения, записи и почтовые сообщения);
- выход в Интернет через программу OpenNet Plus 32 тыс. компьютеров сети Госдепа (май 2003 г.) с использованием системы поиска информации из открытых источников;
- получение доступа к закрытой электронной почте, специальным телеграфным услугам, а также системе «Интелинк» и интернетовской сети отслеживания секретной информации (SIPRNet). Позднее к этой программе подключены все рабочие места (за исключением тех, где обрабатывается несекретная информация и ДСП).

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

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

- обмен информацией и разведданными, как на горизонтальном уровне, так и на вертикальном (федеральные власти, штаты, местные органы);
- проблемы безопасности, связанные с многоуровневым доступом и обменом информации — «несекретной», «чувствительной, но не секретной», «секретной» и «совершенно секретной»;
- консульские услуги — реализация финансируемой Управлением по гражданским делам (УГ Д) Разведывательно-исследовательским бюро (INR) программы TIPOFF, программа контроля за террористами с использованием разведданных ЦРУ, АНБ и ФБР, Система консульской проверки в рамках Межведомственной системы пограничного контроля (IBIS), за работу которой отвечают Служба иммиграции и натурализации (ИНС), а также Таможенная служба. ИНС и УГД обменивается данными в режиме реального времени, в т.ч. о потерянных или украденных загранпаспортах. С 2002 г. ИНС получает данные и фотографии лиц, запросивших неиммиграционные визы во всех своих пунктах въезда. Сотрудник из загранучреждения может иметь доступ к обобщенной базе, где имеется информация по всем выданным и отказанным визам в различных странах мира, о выдаче паспортов и свидетельств о рождении за границей (в рамках системы микрофильмирования паспортных данных). С мая 2002 г. в паспортную службу поступает информация об умерших и находящихся в розыске, планируется ввод данных о преступлениях из ФБР и Налоговой службы.

Как известно из многочисленных заявлений, в т.ч. представителей Госдепа США, в 2006 г. будут введены паспортно-визовые документы с биометрическими параметрами владельцев.

Согласно исследованию консалтинговой компании Forrester Research, к 2003 г. свыше 60% американцев уже хотя бы раз обращались к услугам правительственных сайтов. По прогнозам компании Momentum Research Group, к 2006 г. в Сети будет действовать около 14 000 правительственных программ, с помощью которых будет собираться 15% налогов с населения США на общую сумму 600 млрд долл.

Процесс создания в США ЭП сталкивается с двумя основными проблемами: компьютеры пока имеют не все семьи, а также отставание в темпах информатизации госорганов, в т.ч. из-за нежелания квалифицированных специалистов в области ИКТ поступать на госслужбу.

Кроме того, не все американцы доверяют ЭП. Так, по данным Американской ассоциации информтехнологий (ITAA), 81% американцев обеспокоены возможностью потери их персональной информации на правительственных сайтах, 63% не уверены, стоит ли предоставлять им свою персональную информацию, 72% опасаются использовать электронную цифровую подпись для верификации официальных документов, имеющих юридическую силу.

3.4. Эволюция eEurope

Создание ЭП в странах Европы, как и в других регионах мира, осуществляется в контексте построения информационного общества. В условиях доминирующей роли ЕС в Европе, тем не менее, у каждой страны имеется национальная особенность построения ЭП. Рассмотрим в Европе модель ЭП, рекомендуемую ЕС, ЭП Великобритании и Североевропейскую модель ЭП.

3.4.1. Опыт Евросоюза

Европейское сообщество еще в 1994 году выделило задачу построения информационного общества в число наиболее приоритетных (Europe and the global information society. Recommendations to the European Council, May 1994). В документе было констатировано:

- успешно начата либерализация телекоммуникационного сектора;
- предприняты усилия для обеспечения социальной ориентации информационного общества, поддержки региональных инициатив для достижения согласованного развития;
- сформулирован план действий в области образования;
- оказана поддержка европейской индустрии производства содержания, которая, как ожидается, создаст дополнительно около 1 млн рабочих мест в течение следующих 10 лет;
- успешно воплощены программы научных разработок;
- Европейская комиссия стала важным инструментом выработки общих правил, которые необходимы для перехода к глобальному информационному обществу.

С учетом достигнутого уровня, перед европейскими странами были поставлены следующие новые задачи:

1. Улучшить условия для бизнеса с помощью эффективной и согласованной либерализации телекоммуникаций, создать необходимые условия для внедрения электронной торговли.

2. Необходим переход к обучению в течение всей жизни. В этом направлении работает инициатива «Обучение в информационном обществе».

3. Значительные последствия информационного общества для конкретного человека побудили дискуссию, направленную на то, чтобы поместить людей в центр происходящих преобразований. По результатам обсуждения выпущена «Зеленая книга. Жизнь и работа в информационном обществе: сначала люди» (Green Paper. Living and Working in the Information Society: People First. European Comission, Belgium, 1996). Речь в ней идет о создании новых рабочих мест, охране прав и свобод граждан, прежде всего неприкосновенности личной жизни.

4. Для установления общих правил в этих областях необходимы многосторонние соглашения в рамках ВТО (Europe at the Forefront of the Global Information Society: Rolling Action Plan). Communication from the European Comission to the Council, the Europeean Parliament, the Economic and Social Committee, and the Committee of the Regions, 1996.)

Европейская комиссия в феврале 1995 г. учредила Форум для обсуждения общих проблем становления информационного общества. 128 его членов представляют пользователей новых технологий, различные социальные группы, поставщиков содержания и услуг, сетевых операторов, государственные и международные институты.

Цель работы Форума проследить процесс становления информационного общества в шести областях:

- воздействие на экономику и занятость;
- основные социальные и демократические ценности в «виртуальном сообществе»;
- воздействие на общественные, государственные службы;
- образование, переквалификация, обучение в информационном обществе;
- культурное измерение и будущее СМИ;
- устойчивое развитие, технология и инфраструктура.

Было подчеркнуто, что если Европа не сможет быстро и эффективно адаптироваться, ее ждет не только потеря конкурентоспособности перед лицом США и азиатских экономик, но и рост социального отчуждения внутри европейских стран. В комплексном виде проблемы развития представлены в первом ежегодном докладе Форума «Сети для людей и сообществ» (Networks for People and their Communities. Making the Most of the Information Society in the European Union. First Annual Report to rhe European Commission from the Information Society Forum. June 1996.).

В связи с особой чувствительностью к сбору персональной информации в документах Европейского Сообщества (Building the European Information Society for Us All. First Reflections of the High Level Group of Experts. Interim Report, January 1996) предлагаются следующие рекомендации:

- сбор и хранение идентифицируемой информации должны быть минимальны;
- решение открывать или закрывать сведениях, должно быть предоставлено самим людям;
- при проектировании информационных систем необходимо учитывать необходимость защиты персональной информации;
- граждане должны иметь доступ к новейшим технологиям по защите личной тайны;
- защита персональных сведений и личной жизни должна стать центральным пунктом политики, обеспечивающей право на анонимность граждан в информационных системах.

Цели другой инициативы — ускорить вход школ в ГИО с помощью предоставления им новых средств общения, поощрить широкое распространение мультимедиа в педагогической практике, формировании критической массы пользователей, услуг по производству мультимедийиных продуктов и услуг, усилить европейское образование средствами, присущими ГИО, расширяя культурное и лингвистическое разнообразие (Learning in the Information Society. Action Plan for European education initiative (1996-1998).

Для достижения этих целей было предложено поощрять взаимосвязь региональных и национальных сетей школ на уровне ЕС, стимулировать развитие и распространение образовательного европейского материала, обеспечить обучение и переподготовку для учителей, информировать об образовательных возможностях, которые дают аудиовизуальное оборудование и мультимедийные продукты.

В 2000 г. ЕС принял новую десятилетнюю программу «Электронная Европа» (e-Europe), а также директиву eEurope 2002 Action Plan, согласно которой к 2005 г. в европейских странах должна быть реализована программа создания национальных ЭП.

Ее ключевые цели состоят в следующем:

- обеспечить каждой школе, каждому предприятию, каждому гражданину выход в он-лайновую среду;
- поддерживать распространение европейской культуры через создание «цифровой» литературы, финансирование и развитие новых идей;

- гарантировать социальную направленность информационному обществу, содействовать росту доверия граждан к государству и укреплению социального согласия.

Программа «Электронная Европа» сконцентрирована на следующих 10 сферах:

- наличие доступа в Интернет и к мультимедиа во всех школьных классах;
- удешевление пользования Интернетом;
- ускорение внедрения электронной торговли;
- развитие высокоскоростного доступа для исследователей и студентов;
- использование смарт-карт для безопасности электронного доступа;
- изыскание рискового капитала для малых и средних предприятий, действующих в сфере высоких технологий;
- вовлечение в электронное сообщество нетрудоспособных граждан;
- телемедицина;
- «интеллектуализация» транспорта;
- электронное правительство (e-Government).

Видение ЭП в странах Европы при общей схожести имеет национальные особенности. Так, **Французское правительство** в программе RESO-2007 планирует переход ко второй фазе электронной администрации, состоящей из следующих пяти задач: интеграция телематических служб, прогресс в области защиты персональных данных, укрепление места ИКТ как бытового инструмента, увеличение роли общественных институтов в электронной администрации[18]. Составной частью этой программы является создание для каждого жителя страны собственного персонального портала в Интернет. Эти порталы можно будет использовать, например, для регистрации детей на обучение в школах и уплаты налогов. Эта система называется mon.service-public.fr. и ее создание планируется закончить в 2005 г. Французские власти рассматривают эти порталы как второй этап создания электронного правительства. Первый был начат в 1998 г. и состоял в передаче административных данных в он-лайн. В октябре 2000 г. во Франции был открыт портал service-public.fr. На нем пользователям предлагаются отсылки к сайтам с общественной информацией и предлагается загрузить в он-лайн любую из более чем

[18] См. *Кирия И.В.* Цифровая Республика: Французская модель. Национальные модели информационного общества. – М.: ИКАР, 2004. С. 137–162

1000 официальных форм, справок и т.п. Одной из основных проблем для Web-дизайнеров при создании индивидуальных порталов стало использование электронных подписей. Пока это ПО слишком сложно для подавляющего большинства жителей Франции. Франция также озабочена необходимостью защитить транзакции в Интернет.

В **Италии** порталом «всех итальянцев» с 2002 г. стал www.italia.gov.it. Web-сайты министерств расширяют перечень предоставляемых услуг. Например, портал Министерства социальных дел снабжает жителей различной информацией, в том числе об их правах на пособия и процедурах по усыновлению детей. Кроме того, портал содержит ответы на наиболее часто задаваемые вопросы, чат и электронную почту. Занимая невысокие места по индексу ДЦТ в Европе (позади нее лишь Португалия и Греция), Италия в режиме «догоняющего развития» стала инициатором ряда новых проектов. Один из них — это «e-Government для развития», поддержанный на крупной международной конференции в Палермо в апреле 2002 г.[19]

С видением проблемы ЭП в **Германии** можно ознакомиться на сайте http://www.bund.de/. В сентябре 2000 г. в Германии стартовала программа «Интернет для всех», одновременно была разработана концепция «Инновации и рабочие места в информационном обществе XXI века». Среди ее десяти пунктов особое место занимает «ЭП— инициатива Bund-Online 2005».[20] Особенностью подхода Германии к данной проблеме является развитие широкой сети «электронных городов»[21]. Типичным примером может служить один из сайтов по Берлину[22].

Бюджет **Голландии** 2002 г. четверть всех услуг, предлагаемых правительством, составил в онлайновом режиме. Под этим подразумевается предоставление гражданам информации и услуг госорганов всех уровней посредством Интернет. И уже на первом этапе в ряде стран перевод чиновничьей деятельности в электронную форму стал реальностью. Естественно, что автоматизировать процессы управления на муниципальном и федеральном уровнях легче было там, где и так порядок.

---

[19] См. *Урина Н.В.* Италия: от Anno Domini к Anno Digitals. Национальные модели информационного общества. М.: ИКАР, 2004. С. 113-136.

[20] См. *Вороненкова Г.Ф.* Интернет для всех. Германский путь в «e-society». Национальные модели информационного общества. М.: ИКАР, 2004. С. 50-64.

[21] E-Government – Neue Interessengemeinschaft IEGOV gegrьndet – Golem Network Ne (Электронное правительство – основан новый концерн IEGOV – сеть Golem Network Ne); http://www.itnews.de/0010/10099.html

[22] http://www.e-berlin.de/

За разработку решений для ЭП взялись серьезные местные и международные компании. На крупнейшей международной выставке CeBIT в Германии павильон ENAC Europe (Know-how center for Local & Central Government) с проектами по информатизации деятельности правительств различного уровня все больше заполняется крупнейшими мировыми производителями решений — Microsoft, SAP, Oracle и пр.

Как правило, генеральным подрядчиком выступает крупная и хорошо известная консалтинговая фирма. Так, например, компании Arthur Andersen и Microsoft сформировали альянс по работе с госорганами Эстонии, Латвии и Литвы. В Болгарии создан совет из местных представительств международных компаний Hewlett-Packard, IBM, Microsoft и Cisco Systems. Правда, болгарская ассоциация местных компаний, работающих в области ИКТ — BAIT (Bulgarian Association of IT Companies), — выразила свое неудовольствие, считая, что их интересы тоже надо учитывать при дележе заказов. Систему eProcurement для департаментов и агентств правительства Шотландии (http://www.scotland.gov.uk/) создают английские офисы компаний Cap Gemini Ernst&Young и Elcom International, Inc. По контракту работы растянутся на 7 лет. Cap Gemini Ernst&Young в качестве генподрядчика спланирует и внедрит систему. А Elcom предоставит технологические платформы, в том числе PECOS Internet Procurement Manager и eCommerce Network's Dynamic Trading System.

Анализ показывает, что в Европе так называемый общественный сектор — т.е. комбинация секторов образования, здравоохранения, местные и центральные правительства и связанные с ними предприятия обслуживания — это самый большой заказчик на услуги в области ИКТ. Его объем составляет около 17-18% всего рынка. Эти данные за 2002 г. приводит в обзоре компания IDC.

В абсолютных цифрах в 2000 г. европейский общественный сектор затратил около $1,3 млрд (1,47 млрд евро) на создание и деятельность ЭП (около 6% всех затрат на услуги сферы ИКТ), в 2005 г. (а это год окончания многих проектов в этой области) затраты составят 4 млрд. евро. В 2003 г., как пишет The Register[23], на создание ЭП структур Евросоюза ушло 12% всех средств, выделенных на ИКТ. С 2004 по 2008 год эта доля будет составлять в среднем 10,5%, но вот общая сумма ежегодных расходов на эти цели достигнет 4,2 млрд евро.

Наибольший прогресс в деле построения е-правительства продемонстрировали Великобритания, Норвегия (не член ЕС) и Швеция.

[23] http://www.theregister.co.uk/

В самом низу этого списка — Швейцария. По мнению экспертов IDC, столь слабый, на первый взгляд, показатель одной из богатейших стран Европы объясняется высоким уровнем децентрализации власти в Швейцарии.

Некоторые проекты для более бедных стран финансируются как правительствами самих этих стран, так и Евросоюз. Так, шесть стран юго-восточной Европы (Албания, Кипр, Греция, Югославия, Румыния и Македония) начали совместный проект под названием «eGovernance» (e-government) в целях установления взаимодействия в онлайновом режиме на региональном уровне. Взнос Румынии в рамках этого проекта, например, составил $ 0,5 млн. На начальной стадии проекта создана единая сеть для связи и ряд цифровых библиотек для использования их правительствами и правительственными агентствами. На втором этапе каждый гражданин стран этого региона получит доступ к полезной информации всех стран-участниц для личных или деловых целей.

Основной чертой макроэкономической политики стран ЕС служит поиск определенного баланса между полным контролем со стороны государства и законами рынка, другими словами, сочетание правительственных и рыночных сил с учетом того, что роль каждой из них может меняться в зависимости от сложившейся ситуации. Свое отражение он нашел в отчете датского правительства «Информационное общество 2000», где подчеркивается, что «рынку нельзя позволить взять контроль над стратегией разработки инфомагистралей, однако, эта стратегия должна учитывать возможности рыночных сил»[24]. В то же время ЕС продолжает уделять сегодня большое внимание вопросам приватизации и либерализации рынка ИКТ. Лидирующие позиции в процессе либерализации занимают Великобритания, Швеция, Финляндия, Нидерланды. Так, Великобритания начала свою национальную политику либерализации еще в середине 1980-х гг., либерализация телекоммуникационного сектора в скандинавских странах берет свое начало на рубеже 1980–1990-х гг. Значительный импульс этому процессу придало подписание в феврале 1997 г. 69 странами, представляющими 90 % мирового рынка телекоммуникационных услуг, договора о его либерализации.

Другой, не менее актуальной проблемой, является вопрос, что следует развивать сначала: сети или услуги. **В целом в Европе превалирует мнение, что в первую очередь необходимо развивать сферу услуг**. К числу

[24] *Вершинская О.Н.* Существующие модели построения информационного общества // Информационное общество. 1999. № 3. С. 53.

стран, имеющих противоположный взгляд на эту проблему, относятся Великобритания и Франция. В их планах развития информационного общества указывается, что именно строительство сетей является движущим фактором развития сферы услуг.

Европейская комиссия определила разработку, внедрение и продвижение единого ЭП для объединенной Европы как одно из приоритетных направлений[25].

В 2004 г. страны — члены ЕС и Еврокомиссия подготовили список услуг, которые должны быть доступны гражданам вне зависимости от того, на территории какой страны они находятся.

При этом некоторые панъевропейские сервисы уже начали успешно реализовываться: начал свою работу единый портал для поиска работы во всех сранах Евросоюза[26] (European Job Mobility Portal» **EURES)**, для предоставления единых услуг разработан портал «Твоя Европа» (Your Europe). Этот новый портал базируется на существующих инициативах, таких как Диалог с гражданами (Dialogue with Citizens), Диалог с бизнесом (Dialogue with Business) и портал государственных услуг Евросоюза (Portal of the EU Administration Public-Services.eu), который запущен в пилотном режиме.

Организация по обмену данными между государственными ведомствами (Interchange of Data between Administrations — IDA) недавно опубликовала Стратегический план по разработке единого портала для электронного правительства Европы Public-Services.eu, который станет макетом для обучения и демонстрационных целей до 2005 г., когда произойдет реальное объединение всех существующих электронных сервисов.

На третьей конференции «Государство в XXI веке», состоявшейся 6 апреля 2005 г. в Москве, представителем Microsoft были представлены следующие данные о роли государств по распространению ИКТ в странах Европы.

[25] http://lenta.neweco.ru/ict/878

[26] http://europa.eu.int/eures/

3.4.2. Электронное правительство Великобритании

Среди одиннадцати пилотных проектов, принятых на Брюссельской конференции G7 1995 г., за девятый пункт — развитие ЭП — ответственным была назначена Великобритания (см. 2.3.1.). В Великобритании оно развивается на основе положений «Белой книги по модернизации правительства» (Modernising Government White Paper). Программа называется E-citizen, e-business, e-government. A strategic framework for public service in the Information Age («Электронные граждане, электронный бизнес, электронное правительство. Стратегическая концепция обслуживания общества в информационную эпоху»). Ее основная цель заключается в анализе и конкретизации процесса перехода к правительству информационного века. В программе рассматриваются следующие вопросы[27]:

[27] См. *Дрожжинов В., Штрик А.* Электронное правительство информационного общества. www.pcweek.ru/year2000/n15/cp1251/strategy/index.htm

- структура и состав услуг, которые необходимо реализовать для рядовых потребителей и неправительственных организаций;
- расширение спектра предоставляемых сервисов;
- обеспечение полного охвата граждан и населения правительственными услугами;
- радикальное улучшение использования информации.

Британская программа исходит из того, что трансформация традиционных форм взаимодействия правительства и граждан в цифровую форму не должна стать причиной социального неравенства. Правительство принимает на себя обязательство по уменьшению «цифрового расслоения» общества. Для этого оно проводит целенаправленную политику в области повышения компьютерной грамотности, создания центров обучения и улучшения условий для роста квалификации персонала в области ИКТ, в том числе через обеспечение доступа к национальной сети обучения и к сетевой библиотеке Великобритании. Существует также ряд местных программ в этой области.

Преодоление цифрового барьера, однако, предусматривает не только повышение квалификации населения и решение проблемы доступа к информации. Некоторые граждане не хотят или не имеют возможности стать прямыми пользователями новых технологий, но рассматриваемая стратегия учитывает и эту категорию населения. Новые технологии позволяют улучшить поддержку личных и телефонных транзакций, наряду с организацией интерактивного взаимодействия граждан. Для госорганов основной целью станет освобождение служащих от выполнения рутинных процедур при интерактивных взаимодействиях с населением и обеспечение служащих необходимыми знаниями и оборудованием для успешного выполнения функций промежуточного звена между правительством и гражданами.

Основным правительственным порталом в Великобритании, обеспечивающим работу ЭП, является «Британский сетевой портал для граждан» (UK online Citizen Portal)[28], который обеспечивает доступ к правительственной информации и услугам (с 2001 г.). До этого с 1994 г. информационные услуги оказывал сайт британского правительства, который размещал сайты отдельных правительственных подразделений. Портал имеет выход на сайт Government Gateway, который обеспечивает регистрационные услуги и предоставляет бланки документов (например, налоговые формы). Основной портал дает возможность выхода на сайты коммерческих предприятий, обратную связь, консультации и т. д.

[28] www.open.gov.uk

В наиболее продвинутых системах возникают соответствующие стандарты, например, для известного проекта, реализованного в Великобритании — UK Government Gateway (Шлюз госслужб Великобритании), — выработан специальный стандарт, базирующийся на XML, для обмена данными между разными государственными службами при автоматизации государства. Данный стандарт называется e-GIF (e-Government Interoperability Framework)[29].

Постепенно осознается тот факт, что взаимодействия типа G2G могут проходить в электронной форме не только между ведомствами одного государства, но и между ведомствами разных государств. Некоторые международные организации уже занимаются стандартизацией форматов документов для разных форм межгосударственного взаимодействия, например, UN ECE (United Nations Economic Commission for Europe — Европейская экономическая комиссия ООН) разработала стандарт документов для международной торговли — UNeDocs, также базирующийся на XML. Участниками взаимообмена по UNeDocs могут быть, например, таможенные службы различных государств (хотя этим применение стандарта не ограничивается).

Важно отметить, что на сегодня госпроекты и программы типа e-Country, которые были весьма популярны всего год назад и к которым относится и вполне своевременно появившаяся ФЦП «Электронная Россия», стали общим местом — они существуют и реализуются на тех или иных этапах практически везде, по крайней мере в развитых странах. Например, в рамках осуществляемой британским правительством программы по созданию ЭП, на улицах двух городов — Лондона и Кардиффа в 2005 г. появились интернет-киоски, с помощью которых граждане осуществляют коммунальные платежи и выплачивают штрафы за неправильную парковку.

При этом не стоит обольщаться, что общество в целом так уж радостно принимает эти новации. Во многих странах мира, даже самых успешных в реализации таких проектов, идет достаточно жесткая критика своих правительств. Например, можно процитировать слова из заметки, опубликованной в BBC News[30] относительно уже упоминавшегося проекта в Великобритании UK Government Gateway. Статья называется «Британцы не хотят электронного правительства». В ней правительство критикуется за планы перевести к 2005 г. все свои услуги в он-лайн. В официальных сообщениях утверждается, что к концу 2005 г. 99,9% всех услуг, которые предоставляет правительство Великобритании, будет до-

[29] http://www.e-envoy.gov.uk/publications/frameworks/egif3/contents.htm

[30] www.microsoft.com/rus/government/analytics/egov_evolution.asp

ступно через Интернет. Тем не менее, многие из опрошенных, как утверждают авторы заметки, предпочитают взаимодействовать с госорганами по телефону либо при непосредственном общении, «лицом к лицу».

Ожидается, что к 2008 г., когда цели описанной программы будут достигнуты, ключевые правительственные услуги будут реализованы в электронном виде. Это означает, что наиболее распространенные и типичные процессы взаимодействия правительства с гражданами и бизнесом, например, получение и отправка денег, сбор статистической информации, публикация законов, снабжение, будут реализованы с помощью информационных технологий. Появится широкий спектр медиасредств доступа к правительственному сервису в сфере финансов, розничной торговли, культуры и других областях деятельности. Интернет превратится в централизованную систему, объединяющую непосредственно или через промежуточные звенья персональные компьютеры, цифровое телевидение, средства беспроводного доступа, телефоны и иные приборы с операторами центров вызовов. Услуги центров вызовов могут быть доступными в любое время и из любого места.

По оценкам ЕС, в марте 2005 г. ЭП Великобритании занимало третье место[31]. По прогнозам экспертов, если темпы роста использования Сети в стране останутся на прежнем уровне, Великобритания в скором времени создаст наиболее современное ЭП в мире.

3.4.3. Североевропейская модель

Североевропейские страны, к которым относятся Дания, Исландия, Норвегия, Финляндия и Швеция, последнюю четверть века традиционно занимают лидирующие позиции в инновационной экономике. Одними из первых вступили они и на путь внедрения инфономики. Анализ индекса стран мира доступа к цифровым технологиям (см. 2.1.2.) показывает, что североевропейские страны занимают самые высокие позиции в мире.

По мнению ряда экспертов, ведущие позиции в глобальной конкурентоспособности этих стран обеспечивает их тесное взаимодействие в рамках Северного совета (создан в 1952 г.) и Совета министров северных стран (создан в 1971 г.), а также реализацию этатистской социал-демократической модели социума[32].

---

[31] http://www.webplanet.ru/news/internet/2005/3/9/egov.html

[32] *Смирнов А.* Баренцев-Евроарктический регион: российско-норвежские отношения. Бизнес-Пресс — М, 2002. С.57-58.

В североевропейских странах, наряду с определенными национальными особенностями, отчетливо просматривается общность программных документов по развитию информационного общества, созданию условий для внедрения ИКТ бизнесом, формированию ЭП и электронной демократии, дальнейшему повышению уровня социального развития на основе внедрения ИКТ[33]. При этом у Дании, Финляндии и Швеции, как членов ЕС, естественно, доминируют пункты из программных документов евросообщества. Поскольку парадигма ЭП Евросоюза рассмотрена выше, по данным странам дается лишь краткая информация об особенностях создания ЭП.

3.4.3.1. Дания

Отличительная особенность подхода Дании к созданию ЭП заключается в том, что в настоящее время в этой стране более быстро, чем в других североевропейских странах, осуществляется переход от государственного регулирования рынка ИКТ к его либерализации. 17 мая 2002 г. Министерство науки, техники и инноваций заключило с компаниями Microsoft и Accenture контракт, открывающий новую страницу в использовании веб-служб XML (XML Web Services) для ЭП в госорганах.

Реализация данного проекта предусматривает создание следующих основных элементов:

- единого и централизованного хранилища XML-схем, представляющего собой «электронный словарь», которым могут пользоваться все желающие;
- виртуальных рабочих областей, где частные и государственные организации смогут вести постоянную совместную работу по созданию и расширению «электронного словаря» в онлайновом режиме;
- места для публикаций расширений «электронного словаря» и вэб-служб XML. Там же Датский комитет по использованию XML (Danish XML Committee) сможет осуществлять стандартизацию этих ресурсов с целью облегчения интеграции государственных и частных организаций;
- организации уведомления обо всех изменениях в схемах, чтобы все пользователи были заранее сориентированы о модификациях;

[33] Е.Вартанова. Северная модель: государства всеощего информационного благоденствия? Национальные модели информационного общества. –М.:ИКАР.2004.С.84.

- рассылки новостей о вэб-службах на базе XML и ряда общих норм по созданию XML-схем и веб-служб XML в Дании.

При отсутствии базы XML-Infostructurebase каждому госоргану при попытке интеграции с какой-либо другой стороной пришлось бы начинать работу с нуля. Окончательный вариант XML-Infostructurebase в виде вэб-узла стал доступен для всеобщего пользования в марте 2003 г. и был размещен в Интернете датским партнером-субподрядчиком — компанией DMdata. Таким образом, были созданы огромные возможности для реализации интеграционных решений в госсекторе Дании. Не без влияния данного фактора электронное правительство Дании в рейтинге ЕС заняло седьмое место[34].

3.4.3.2. Исландия

По оценкам экспертов Евросообщества ЭП Исландии[35] занимало 8 место, однако имело самый лучший прогресс за 2004 г.[36] Наиболее развитыми онлайновыми сервисами оказались те, что способствуют пополнению казны: например, онлайновое заполнение налоговых деклараций. А такие услуги, как получение лицензий и прочая «разрешительная документация», не приносящая существенных дивидендов государству, остается, как и в ЭП других стран, на сравнительно отсталом уровне.

3.4.3.3. Норвегия

Норвегия не входит в ЕС, однако норвежские власти не только используют все программы ЕС, но и в некоторых компонентах внедрения ИКТ опережают страны — члены ЕС. Об этом убедительно говорит индекс Норвегии по данным МСЭ, приведенный во второй главе.

Переход от экономики, в значительной степени базирующейся на эксплуатации сырьевых ресурсов, к новой экономике, основу которой составляет высокотехнологичное производство, является приоритетной задачей правительства Норвегии. Норвежское правительство считает, что повышение конкурентоспособности норвежских компаний может быть достигнуто реализацией следующих мер:

- упрощением процедур представления отчетов хозяйствующими субъектами органам власти на основе использования ИКТ;

---

[34] http://www.webplanet.ru/news/internet/2005/3/9/egov.html

[35] Население страны около 300 тыс.чел.

[36] http://www.webplanet.ru/news/internet/2005/3/9/egov.html

- расширением использования широкополосных информационных сетей и их доступностью для всех.

Создание необходимой для этого материальной инфраструктуры должно быть обеспечено за счет использования механизмов конкуренции с осуществлением мер государственной поддержки в отношении тех регионов и групп населения, которым услуги широкополосных сетей связи будут предлагаться рынком по недоступным ценам;

- либерализацией рынка услуг ИКТ в рамках ВТО с тем, чтобы усилить возможности роста отраслей норвежской экономики, продукция которых ориентирована на экспорт;
- укреплением госполитики в области ИКТ путем повышения уровня согласованности действий органов исполнительной власти;
- расширением электронной торговли.

Функции координирующего органа в этой сфере возложены на Министерство экономики и торговли. Норвегия занимает лидирующие в мире позиции в области электронной торговли и ведения коммерческой деятельности с использованием ИКТ. Так, программа VeRDI (в переводе с норвежского языка — стоимость) осуществляется под эгидой Государственного фонда экономического и регионального развития. Эта программа призвана способствовать расширенному внедрению электронной торговли мелкими и средними предприятиями[37] и является общедоступным порталом для получения информации, относящейся к электронной торговле. Норвежские власти заинтересованы в стимулировании электронной торговли путем создания электронной биржи для проведения госзакупок. Министерством экономики и торговли Норвегии учрежден Форум по электронной торговле, который также содействует укреплению диалога между коммерческими и властными структурами, выступая в качестве консультанта по важнейшим вопросам. Расширение электронной торговли, электронной коммерции и других форм электронного взаимодействия зависит, в том числе, от решений в плане оплаты приобретаемых услуг, защиты информации о личности, охраны коммерческой тайны и признания с точки зрения гражданского права электронных сделок наравне со сделками, оформленными на бумажных носителях. Свобода заключения контрактов, включая свободу выбора формы, является базовым положением норвежского законодательства. Принцип о свободе выбора формы состоит в том, что стороны сами определяют, в какой форме будет заключен контракт: устной, письменной или электронной. Форма контракта сама по себе не имеет значения при-

[37] www.handel.no

менительно к тому, что контракт является обязательным для исполнения сторонами. Таким образом, ничто не препятствует тому, что суды могут принимать при рассмотрении дел электронные доказательства.

Власти Норвегии целенаправленно работают над гармонизацией правовых актов, приводя их в соответствие с потребностями ИКТ-общества и создавая тем самым условия для более широкого использования средств электронной коммуникации, в том числе путем устранения имеющихся в этой сфере препятствий в нормативных актах.

Увеличение обществом потребления услуг ИКТ -сектора ведет к тому, что информационные системы, как часть коммерческой, управленческой или частной сферы, становятся все уязвимее для несанкционированных действий. Исходя из этого, правительство Норвегии реализует мероприятия, повышающие информбезопасность, как государства, так и частных лиц. Далее, системы, жизненно важные с точки зрения обеспечения национальных интересов и во все большей степени зависимые от ИКТ-сектора, могут быть выведены из строя в результате отказа СВТ, если не принять соответствующих мер безопасности. Норвежские власти обеспечивают информбезопасность решением двух вопросов:

- предотвращение несанкционированного проникновения в информсистемы;
- создание надежной инфраструктуры для электронного взаимодействия в сфере госуправления и коммерческой деятельности. В этих целях используются закрытые сети[38].

Правительство Норвегии разработало национальную стратегию в области информбезопасности. В бюджете 2002 г. имелся раздел «Специальные меры в области информационных технологий», который включает:

1. Центр информационной безопасности — 4,5 млн крон (600 000 долл.);
2. координацию ИКТ-политики — 7,9 млн крон (более 1 млн долл.);
3. создание высокоскоростных коммуникаций 65,9 млн крон — 8,8 млн долл.

Норвегия стремится стать активным участником ГИО. Исходя из политики в области электронной торговли, программа участия сформулирована в следующих четырех положениях:

[38] Закрытость может в ряде случаев обеспечивать повышенную безопасность и уменьшать потребности в установлении общих правил взаимодействия, однако увеличивает расходы.

- упростить открытие предприятий электронной торговли и ведение электронной коммерческой деятельности;
- делать ставку на развитие опыта и профессиональных знаний в этой сфере;
- создать условия для ведения предпринимательской деятельности, всесторонне ориентированной на охрану окружающей среды;
- создать условия для использования норвежской экономикой возможностей глобализации мирохозяйственных связей на основе использования достижений ИКТ сектора.

При этом основными компонентами регулирования электронного рынка являются следующие вопросы:

- электронный маркетинг и извещение о закупках;
- заключение контрактов в электронной форме;
- электронно-цифровая подпись;
- оплата в электронной форме.

Норвежский опыт использования ИКТ очень интересен для России по следующим причинам:

1. Норвегия и России не являются членами ЕС.
2. Норвегия перешла к инфономике от «ископаемой» экономики. При этом внедрение ИКТ резко увеличивает конкурентоспособность на мировых рынках углеводородной, рыбной и иной норвежской продукции.
3. Норвегия, как сосед России, участвует в ряде региональных организаций (Совет государств Балтийского моря, Совет Баренцева/Евроарктического региона, Арктический совет и т.д.), куда входит и Россия или ее субъекты (республики Карелия, Коми, Архангельская и Мурманская области). В рамках различных программ сотрудничества особо выделяются проекты по сотрудничеству в ИКТ сфере (телемедицина, Баренцев виртуальный университет, экомониторинг, внедрение скоростного Интернета, информатизация органов местной власти и т.д.).

3.4.3.4. Финляндия

Успех Финляндии и финских компаний в сфере ИКТ является результатом долгосрочной, целенаправленной государственной политики. Еще в начале 90-х гг., т.е. практически в одно время с США, в стране велись интенсивные исследования, нацеленные на создание национальной информационной стратегии[39]. Следует напомнить, что

[39] См. *Химанен П., Кастеллс М.* Информационное общество и государство благосостояния: Финская модель. — М., 2002.

в этот период Финляндия переживала серьезный экономический кризис, вызванный в т.ч. и распадом СССР — традиционного торгового партнера Suomi.

В 1995 г. были опубликованы результаты исследований, а также отчеты министерств: «Описание национальной политики развития информационных сетей 1995–1998 гг.», «Финский путь в информационное общество» и «Информационная стратегия в области образования и научных исследований». На их основе министерства подготовили планы действий, а Министерство финансов организовало Комитет национального информационного общества и Форум информационного общества, которые приступили и к созданию ЭП. Министерство образования разработало культурную программу информационного общества и предложение по созданию национальной электронной библиотеки. Министерство транспорта и связи сконцентрировало усилия на создании технических предпосылок и охране сетевых услуг.

Результаты исследований в области информационного общества и ЭП были опубликованы компанией Sitra, Финским национальным фондом исследований и разработок и Министерством образования. Отчет «Строительство будущего Финляндии с учетом безопасности и широких возможностей» содержит вывод, что такая однородная страна, как Финляндия, имеет конкурентные преимущества в продвижении к информационному обществу и созданию ЭП. В отчете подчеркивается, что внедрение ИКТ должно обеспечить лучшее будущее для каждого жителя Финляндии. Sitra ищет возможности для строительства лучшего будущего в Финляндии за счет проведения исследований, обучения, внедрения инноваций и корпоративного финансирования. Имеющиеся у компании Sitra финансовые ресурсы позволяют ей оперативно принимать решения. В апреле 1999 г. Министерство образования опубликовало переработанный меморандум «Национальная стратегия на 2000 — 2004 гг., образование, обучение и исследования в информационном обществе». Этот меморандум нацеливал на то, чтобы к 2004 г. в стране было создано «общество знания»[40].

В последние годы многие страны Евросоюза последовали примеру Финляндии в динамичном развитии инфраструктуры обмена данными и дерегуляции сектора телекоммуникаций. Результаты впечатляющие: в 2001 и в 2003 гг. Финляндия признавалась ООН самой развитой страной в сфере ИКТ и комфортности жизни[41].

---

[40] http://virtual.finland.fi/

[41] *Вартанова Е.* Северная модель: государства всеобщего информационного благоденствия? Национальные модели информационного общества. — М.: ИКАР, 2004. С. 107.

3.4.3.5. Швеция

Швеция — одна из самых передовых стран Европы в области развития услуг ЭП[42]. Рынок программного обеспечения для госсектора в Швеции продолжает расти, несмотря на некоторый экономический спад. Ожидается, что к 2007 г. рынок вырастит со 186 млн евро до 306 млн евро. Интересно то, что первая стадия построения ЭП — создание порталов для граждан и бизнеса в Швеции уже пройдена, однако многое еще предстоит сделать для достижения высшего уровня ЭП — «бесшовного контакта» граждан с правительством.

По мнению экспертов, будущее ЭП в Швеции — это дальнейшее развитие автоматизированных и комплексных услуг. Согласно отчету компании IDC, рынок ЭП будет увеличиваться с темпом не менее 25% в год.

3.5.Восточная модель

Достаточно условно эксперты выделяют две основные модели развития информационного общества и электронных правительств: западную и восточную. Причем в рамках западной модели мы уже отделили путь, выбранный Европой, от американского пути, а в рамках восточной модели особое место занимает Китай (КНР).

Западная модель рассмотрена выше. В Азиатско-Тихоокеанском регионе данными вопросами активно занимается Азиатско-Тихоокеанский экономический союз (АТЭС). Для стран арабского мира большое значение имеет международная неправительственная организация RAITNET — Региональная арабская сеть информационной технологии.

Представители восточной модели стремятся разработать альтернативный западному подход, который базируется на утверждении собственных ценностных ориентаций в отношении индустриализации, информатизации и социального развития. В его основе лежат сотрудничество государства и рынка, попытка установить связь между культурными ценностями, свойственными конфуцианству, и происходящими социальными изменениями. Философские постулаты сосуществования и сопроцветания, а также содействие государства в реализации этих принципов на уровне отдельной организации является, по мнению азиатских политиков, залогом успеха. **В рамках восточной модели выделяются Япония, «азиатские тигры», определенные сдвиги по созданию ЭП наметились в Китае, Индии.**

[42] http://neweco.ru/

3.5.1. Япония

Понятие «японское экономическое чудо» стало хрестоматийным. Успехи страны в развитии ИКТ в целом сопоставимы сегодня с успехами в этой области США. Одним из важнейших факторов их достижения остаются значительные расходы на научные исследования и разработки, высокий приоритет ИКТ в решении проблем социально-экономического развития страны. После Второй мировой войны страна была разрушена: выпуск промышленной продукции в 1946 г. не достигал 15% от довоенного уровня, безработица превышала 10 млн человек, реальная зарплата составляла лишь 13% от довоенной.

Финансовая стабилизация, осуществленная американским эмиссаром Дж. Доджем в 1949–1950 гг., выровняла цены с мировыми и позволила отменить нормирование продуктов. К 1955 году Япония вступила в МВФ и ГАТТ. Одним из приоритетных направлений в программах страны становится развитие электротехнической и электронной отрасли, создается Комитет по компьютерным исследованиям. Начиная с 1964 г. было начато производство компьютеров, создано Управление развития информационной технологии, предоставлявшее займы для образования компаний, разрабатывавших программное обеспечение. В итоге к 1970 г., последовательно обойдя Италию, Англию, Францию и ФРГ, Япония вышла на второе после США место в капиталистическом мире по объему ВНП[43]. Страна становится мировым лидером в производстве телевизоров, радиоприемников и т.п. Знаком признания японского «экономического чуда» стало избрание Осаки местом Всемирной выставки 1970 года.

Стратегическими целями страны в сфере информатизации стали: построение наибольшего числа взаимосвязанных и совместимых телекоммуникационных сетей, разработка информационных устройств и технологий, развитие программного обеспечения и информационных услуг, подготовка квалифицированных кадров для работы в ИКТ. Провозглашение и последующая реализация этих целей послужили огромным стимулом для бурного развития информационно-ориентированной деятельности в Японии. Следуя примеру развитых стран Западной Европы и США, страна смогла добиться блестящих результатов в адаптации импортных технологий, и сегодня ее главным при-

[43] За 1955–1970 гг. экономического «чуда» среднегодовой прирост ВНП в Японии превышал феноменальные 11%, при этом норма накопления приближалась к 35%. В 1988 г. ее ВНП на душу населения превысил американский аналог, а в 1990 г. его прирост составил около 6%, тогда как в самой развитой стране мира не достиг и 1%.

оритетом становится собственное производство нового знания, технологий и новых продуктов. Активно развивается Интернет-сервис, сетевой рынок «бизнес — бизнесу» (B2B), виртуальные магазины, появляются новые формы банковских и финансовых услуг, страна создала средства мобильной связи третьего поколения (3G) и вплотную подошла к созданию четвертого поколения. По прогнозам Агентства планирования экономики Японии, внедрение ИКТ повысит реальный ВВП страны примерно на 6% в ближайшие три года. Для Японии из-за низкой рождаемости характерно старение населения. За счет внедрения новейших ИКТ, в т.ч. в ЭП, планируется компенсировать отрицательное влияние на экономику уменьшения численности трудоспособного населения.

В основе деятельности ЭП **«азиатских тигров»** лежит так называемая модель экономического сотрудничества государства и рынка. Успех этих стран базируется, в частности, на вмешательстве государства в принятие решений в области крупных вложений частного капитала, на активном участии государства в создании национальной информационной инфраструктуры и ЭП. К проблемам информационного развития, по которым правительства высказывают особую озабоченность, относятся постоянно растущая конкуренция в области производства и внедрения новейших ИКТ и связанная с этим потенциальная возможность потери какого-то сегмента рынка или рабочих мест, а также проблема обеспечения равного доступа к информационным ресурсам.

3.5.2.Сингапур

Особого внимания среди «азиатских тигров» заслуживает Сингапур, где были разработаны следующие программы[44]:

- Компьютеризации госслужбы (1981 г.);
- Национальный план по ИКТ (1986 г.);
- Стратегический план «ИТ-2000» «Интеллектуальный остров» (1991 г.);
- «Основной план по ИКТ 21» (2001 г.) на 10 лет.

ЭП Сингапура — самое развитое после ЭП США и Канады — нацелено на выполнение следующих пяти стратегических целей:

- перестроить правительство к инфономике;

[44] См. *Ткачева Н.В.* Сингапур: социальные измерения информационного общества. Национальные модели информационного общества. — М.: ИКАР, 2004. С. 226-234.

- доставлять интегрированные электронные услуги;
- быть упреждающим и отзывчивым правительством;
- использовать ИКТ для открытия новых возможностей;
- быть инноваторами с помощью ИКТ.

Для реализации целей развития ЭП Сингапура в 2000 г. был разработан «План действий правительства» с бюджетом 1,5 млрд долл.США. Этот план включает в себя стратегические цели и стратегические программы ЭП. Всего определено шесть стратегических программ достижения вышеперечисленных стратегических целей ЭП Сингапура:

- Основанная на знаниях рабочая среда: госслужащие на всех уровнях должны уметь использовать преимущества ИКТ для улучшения рабочих процессов, доставки услуг и работы в команде.
- Электронная доставка услуг: все правительственные услуги, которые технически могут быть оказаны электронным образом или для улучшения качества которых могут быть использованы электронные каналы, должны быть оказаны соответственно.
- Технологические эксперименты: они будут способствовать более быстрому приспособлению государственных органов к быстро изменяющимся техническим условиям и снизят вероятность крупных инвестиций в неверные решения.
- Улучшение оперативной эффективности: компьютерное оборудование должно быть современным.
- Адаптирующаяся ИКТ-инфраструктура: конвергенция телекоммуникаций, радио-технологий и информтехнологий открыла возможности для ЭП с более низкими издержками.
- Образование в сфере ИКТ: образовательные программы в сфере ИКТ дают знания не только в изучении компьютерных систем и приложений, но и в использовании ИКТ для улучшения рабочих процессов и доставки правительственных услуг.

«Правительственный портал» (Singapore Government Online) в 2005 г. приблизился к высшему «бесшовному» уровню ЭП. На третьей конференции «Государство в XXI веке», состоявшейся 6 апреля 2005 г. в Москве, представителем Microsoft был представлен следующий пример эффективности от внедрения элементов ЭП. Получение экспортной лицензии в Сингапуре ранее требовало заполнения 21 формы, и это занимало 3 недели. После создания ЭП онлайновая форма подтверждается в течение 15 секунд[45]!

По оценке экспертов дальнейшее развитие ЭП Сингапура потребует значительной координации на всех уровнях госуправления.

[45] http://www.pcweek.ru/?ID=300257

3.5.3.Южная Корея

Опыт Южной Кореи по созданию ЭП заслуживает пристального внимания.

Так, в конце 80-х гг. был реализован проект информатизации государства (National Basic Information Sistem Project), в середине 90-х гг. была создана программа «Корейской информационной инфраструктуры» (Korea Information Infrastucture Initiative). Характерно, что рывок в развитии ИКТ Корея совершила в условиях экономического кризиса 1997 г., и быстрый выход из него, по мнению экспертов, был бы невозможен без развитого сектора ИКТ.

Согласно программе «Корейская информационная инфраструктура» правительство поддерживает реализацию двух проектов, один из которых связан с созданием ЭП Кореи, а в центре внимания второго, носящего название «CYBER KOREA 21» (1999–2002 гг.), — вопросы, связанные с перспективами развития в стране пользовательского Интернета. Следует отметить, что сроки создания первого проекта для ЭП были скорректированы с 2015 г. на 2005 г.[46], т.к. уже в 2003 г. начал функционировать портал «Корейское электронное правительство» с сервисом «Правительство для граждан»[47]. Портал Korean Electronic Government использует единую информационную систему, охватывающую все административные учреждения и позволяет послать запросы по 393 основным задачам (таким как, например, выдача справок о регистрации по месту жительства, об официальной стоимости земельных участков и т.д.), получить сведения из огромной базы данных, охватывающей порядка 4 тысяч категорий рубрик. Кроме того, за счет использования данной системы около 20 видов документов выдаются в любом административном офисе, что позволяет гражданам не совершать длительные поездки для их получения. Эта полностью интегрированная Интернет-служба стала первой подобной системой в мире. Позднее к данной онлайновой системе стало возможным обращаться через сотовые телефоны и PDA-устройства, в т.ч. и к ее английской версии[48].

По оценке экспертов, бурный рост ИКТ явился следствием того, что государство активно включает ИКТ-технологии в планы развития страны, избегая при этом прямого вмешательства и считая технологии

---

[46] См. *Ткачева Н.В.* Основные тенденции развития информационного общества в Южной Корее. Национальные модели информационного общества. — М.: ИКАР, 2004. С.235-245.

[47] https://www.egov.go.kr/default.html

[48] http://www.tradecenter.ru/NewsAM/NewsAMShow.asp?ID=51333

приоритетным направлением развития. Важным шагом правительства стало принятие закона «О цифровом разрыве» (2000 г.), который стимулировал направление средств в НИОКР, улучшение инфраструктуры и автоматизацию, а также на освоение цифровых технологий в обществе в целом. При этом правительство предпринимает активные шаги по созданию конкурентной среды и вследствие этого достигает снижения цены на большинство сервисов. В силу этого сегодня ИКТ-промышленность Кореи занимает лидирующие позиции в мире.

Как уже отмечалось (2.1.), в ООН Южную Корею поставили на весьма высокое место в глобальном рейтинге готовности к созданию ЭП. По этому показателю США заняли 1-е место с 3,11 балла. Второе место заняла Швеция, следом за которой идут Австралия, Новая Зеландия, Сингапур и другие государства. Корея, наряду с Испанией заняла 13-е место, набрав 2,3 балла.

Газета Wall Street Jornal называет жителей Кореи самыми «продвинутыми» интернетчиками[49]. В Корее в 2004 г. насчитывалось свыше 30 тыс. интернет-кафе, возможностями онлайн-бирж пользовались более 70% корейцев, около 15 млн жителей этой страны (из 47,5 млн.) осуществляют банковские операции через Интернет. Среднестатистический кореец в течение месяца (2003 г.) проводил в Интернете около 17 часов, в то время как его «сосед по региону» — японец — почти вдвое меньше[50].

Южная Корея активно осуществляет программу международного сотрудничества. С ее помощью создаются ЭП в Индии, Казахстане, Кыргызстане, Мексике, Таиланде и др. странах[51]. Южная Корея все отчетливее позиционирует себя как самый мощный информационный коммуникатор (HUB) всей Азии.

3.5.4. Китай

Согласно докладу американской финансовой и инвестиционной компании Morgan Stanley Dean Witter (январь 2001 г.) Китай вошел в тройку по потенциалу роста отрасли ИКТ (1-е место у США, 2-е — у Японии, 4-е — у Германии, 5-е — у Великобритании, 6-е — у Южной Кореи)[52].

---

[49] www.dialog-21.ru/full_digest.asp?digest_id=14822 (23 КБ)

[50] См. также *Астафьев А.В.* Интернет в повседневной жизни Южной Кореи. Национальные модели информационного общества. – М.: ИКАР, 2004. С. 246-250.

[51] http://www.cnews.ru/newsline/index.shtml?2004/08/10/162199

[52] См. *Лежун Цзя.* Китайский Интернет: стратегия информатизации и телекоммуникационная политика. Национальные модели информационного общества. – М.: ИКАР, 2004. С. 251-262.

Национальная стратегия информатизации страны началась в 1983 г., когда ИКТ были включены в общую государственную программу. В 1986 г. ИКТ опять вошли в перечень высоких технологий по программе «863». В 1993 г. был введен в действие ряд важных объектов ИКТ. В 1996 г. был утвержден «Доклад о девятом пятилетнем плане национальной экономики и социального развития и перспективных целях до 2010 г.», в котором развитию ИКТ уделено особое внимание.

Для реализации планов в 1998 г. были реорганизованы органы госвласти, ответственные за ИКТ, в 2000 г. было принято «Положение о телекоммуникации в КНР», в 2001 г. Госсоветом была утверждена телекоммуникационная реформа (не без влияния вступления Китая в ноябре 2001 г. в ВТО).

Весомые инвестиции китайского правительства в сферу научно-технических разработок, привлечение иностранного капитала уже приносят свои плоды, обещая в будущем превратить эту некогда технически отсталую страну в один из мировых центров новых технологий. В первую очередь речь идет о секторе телекоммуникаций. Совокупный объем инвестиций в эту сферу, согласно статистическому отчету китайского правительства, превысил в 2003 г. 45 млрд долл. Сейчас Китай занимает второе место в мире по размеру своих коммуникационных сетей[53]. Обусловлено это и заинтересованностью самого мирового топ-менеджмента в громадном и быстро растущем рынке Китая. По предварительным оценкам, объем инвестиций в научно-исследовательскую сферу Китая со стороны транснациональных корпораций достигает 5 млн долл. в год. С привлечением иностранного капитала в стране открыто более 140 научных центров. Китайские специалисты, возвращающиеся после учебы на родину, также являются мощным двигателем в развитии китайского сектора новых ИКТ. К примеру, лишь в провинции Чжунгуаньцунь, расположенной на северо-западе Пекина и известной как «китайская силиконовая долина», большинство компаний возглавляют получившие образование за границей китайцы.

В Китае создаются элементы ЭП, которые, однако, в условиях госрегулирования Интернет-контента значительно отличаются от ЭП по западной модели.

---

[53] Китай становится мировым центром хай-тека — http://www.nsda.ru/home.asp?artId=479

3.5.5.Индия

Индия не выбрала ни пути полной приватизации, ни пути мягкой либерализации. Ее модель называют промежуточной. Государственные предприятия не передаются в частный сектор, а конкуренция разрешается на рынке местных услуг, при этом допускается 49 % иностранного присутствия[54]. Междугородняя и международная связь продолжают оставаться в руках государства. Своим главным капиталом на пути в ГИО Индия считает свои человеческие ресурсы. Индия имеет третий по величине после США и России научно-технический потенциал в мире. Вузы страны ежегодно выпускают свыше 115 тыс. инженеров и 40 тыс. менеджеров, из этой армии специалистов около 50 тыс. человек каждый год отправляются работать за границу. Многие из них, набравшись конкретного опыта и практических знаний, возвращаются на родину, где уже созданы мощные технопарки.

Программисты-индусы, согласно опросу, проведенному консалтинговой фирмой Meta Group, уверенно держат пальму первенства по продуктивности и приносимой ими компаниям прибыли. В будущем правительство намерено превратить страну и в крупного экспортера ИКТ. Следует отметить, что еще в 1996 г. 100 из 500 крупнейших американских фирм приобретали программное обеспечение в Индии[55]. Сотрудничество Индии, в т.ч. с Южной Кореей по созданию ЭП приносит существенные результаты. Индию сегодня никак нельзя в данном вопросе отнести в разряд аутсайдеров.

Вместе с тем Индия остается одной из беднейших стран мира. С одной стороны, программисты высшей квалификации, с другой — миллионы людей, никогда в своей жизни не видевшие компьютера. Таким образом, речь пока идет об определенных успехах Индии, но на очень перспективных направлениях.

---

[54] *Вершинская О.Н.* Существующие модели построения информационного общества // Информационное общество. 1999. № 3. С. 57.

[55] Там же. С 58.

ГЛАВА 4
ИНФОРМАЦИОННОЕ РАЗВИТИЕ — ПУТЬ КОНКУРЕНТОСПОСОБНОЙ РОССИИ

Умные стремятся владеть информацией,
мудрые — результатом ее обработки.

4.1. Основополагающие подходы России к формированию информационного общества

Практически сразу после появления в мировой практике различных концепций по формированию информационного общества, в России также были предприняты попытки сформулировать отечественные пути по его созданию. Наиболее заметными из них стали следующие.

4.1.1. Концепция государственной информационной политики

Концепция государственной информационной политики была разработана в 1998 г., одобрена Комитетом по информационной политике и связи Государственной Думы Федерального Собрания Российской Федерации 15 октября 1998 г. и Постоянной палатой по государственной политике Политического консультативного совета при

Президенте России 21 декабря 1998 г., опубликована в 1999 г. и разослана во все органы государственной власти на федеральном уровне и уровне субъектов Федерации.[1] В ней провозглашены следующие базовые принципы государственной информационной политики:

- принцип открытости — все мероприятия информполитики открыто обсуждаются обществом, и государство учитывает общественное мнение;
- принцип равенства интересов — политика в равной степени учитывает интересы всех участников информационной деятельности, вне зависимости от их положения в обществе, формы собственности и гражданства;
- принцип системности — при реализации тех или иных решений должны учитываться их последствия для всех объектов и субъектов, затрагиваемых этими решениями;
- принцип приоритетности производителя — при равных условиях приоритет отдается отечественному производителю ИКТ, продуктов и услуг;
- принцип социальной ориентации — основные мероприятия государственной информполитики должны быть направлены на обеспечение социальных интересов общества;
- принцип государственной поддержки — мероприятия информполитики, направленные на информразвитие социальной сферы, финансируются преимущественно государством;
- принцип приоритетности права — развитие и применение правовых методов имеет приоритет перед экономическими и административными решениями проблем информационной сферы.

4.1.2. Концепция формирования информационного общества в России

Концепция была одобрена 28 мая 1999 г. межведомственной Госкомиссией по информатизации при Госкомитете России по связям и информатизации[2]. Содержание Концепции отражают ее разделы:

- предпосылки перехода России к информационному обществу;
- цель Концепции;
- ее базовые положения;

---

[1] *Артамонов Г.Т., Кристальный Б.В., Курносов И.Н. и др.* О концептуальной базе построения в России информационного общества // Информационное общество. 1999. № 9. С. 17-19.

[2] http://www.iis.ru/library/riss/riss.ru.html#000

- особенности и возможные пути перехода России к инфообществу;
- социально-культурные обоснования выбранного пути;
- основные направления реализации перехода к инфообществу;
- первоочередные задачи госполитики перехода к инфобществу.

Цель Концепции – определение российского пути построения инфообщества, основных условий, положений и приоритетов госинформполитики, обеспечивающих его реализацию. К характерным чертам и признакам этого пути отнесено:

- формирование единого ИКТ пространства России как части мирового информпространства, полноправное участие в процессах интеграции регионов, стран и народов;
- становление и в последующем доминирование в экономике новых технологических укладов, базирующихся на массовом использовании ИКТ, средств вычислительной техники и телекоммуникаций;
- создание и развитие рынка информации и знаний как факторов производства в дополнение к рынкам природных ресурсов, труда и капитала, переход информресурсов общества в реальные ресурсы социально-экономического развития, фактическое удовлетворение потребностей общества в информационных продуктах и услугах;
- возрастание роли инфраструктуры ИКТ в системе общественного производства;
- повышение уровня образования, научно-технического и культурного развития за счет расширения возможностей систем информобмена на международном, национальном и региональном уровнях и, соответственно, повышение роли квалификации, профессионализма и способностей к творчеству как важнейших характеристик услуг труда;
- создание системы обеспечения прав граждан и социальных институтов на свободное получение, распространение и использование информации как важнейшего условия демократического развития.

В Концепции отмечено, что в России сформировались следующие факторы развития, которые можно рассматривать как предпосылки перехода к инфообществу:

- информация становится общественным ресурсом развития, масштабы ее использования стали сопоставимыми с традиционными (энергия, сырье и т.д.) ресурсами;
- сформировался и успешно развивается отечественный рынок телекоммуникаций, ИКТ продуктов и услуг;
- в стране растет парк ЭВМ, ускоренными темпами идет развитие систем и средств телекоммуникации;

- в значительной степени информатизированы многие отрасли хозяйства, банковская сфера и сфера государственного управления;
- в обществе складывается понимание актуальности задачи перехода к инфообществу с политической и экономической точек зрения;
- Россия является частью мирового политического и экономического сообщества в такой степени, в какой она никогда не была в прошлом;
- сформирована и функционирует госструктура, ответственная за создание и развитие ИКТ базиса обеспечения процессов перехода.

Из базовых положений концепции заслуживают внимания следующие:

- стратегической целью перехода к инфообществу является создание развитой среды ИКТ и интеграция России в ГИО, что должно обеспечить существенное повышение качества жизни населения и социально-политическую стабильность общества и государства;
- переход к инфообществу должен рассматриваться как необходимое условие выхода страны из экономического кризиса, как инструмент преодоления трудностей социальной, политической и духовной жизни, как фактор интеграции общественного сознания вокруг непреходящих гуманистических ценностей и национально-исторических традиций народов России;
- переход к инфообществу полностью отвечает **концепции устойчивого развития** — формированию экономики, основанной на знаниях, а не на расширяющемся потреблении природных ресурсов, сокращению отходов производства, решению экологических проблем, приобщению к благам техногенной цивилизации.
- Государство играет ведущую роль в обеспечении процесса перехода к инфообществу за счет:
  - —координации деятельности различных участников этого процесса;
  - —сохранения в своих руках политических, экономических и правовых механизмов, определяющих «правила игры» для участников процесса;
  - —создания адекватной новым условиям законодательной и нормативно-правовой баз, форм и методов регулирования, способствующих инвестициям и развитию конкуренции;
  - —привлечения к активному участию в процессе перехода частного сектора экономики;

— предоставления свободы выбора направлений деятельности предпринимательским структурам, заинтересованным в развитии производства и отечественного рынка ИКТ, продуктов и услуг.

- В условиях отсутствия у государства мощных финансовых рычагов, основными средствами госрегулирования и контроля за процессами перехода остаются законодательная и нормативно-правовая базы, регулирующие информационные отношения в обществе.
- На начальном этапе государство берет на себя основные расходы. При этом предполагается, что значительные финансовые ресурсы поступят от населения в виде оплаты предоставляемых ИКТ и услуг связи.

Государство выступает катализатором происходящих перемен в интересах развития общества и личности. С этой целью оно:

— ведет борьбу с монополизмом и осуществляет контроль за концентрацией собственности в СМИ и ИКТ бизнесе;

— юридически и технологически обеспечивает права на доступ к информации и информресурсам для всего населения, а также охрану персональных данных, гарантирует гражданам предоставление постоянно расширяющегося набора информуслуг (телефонная связь, электронная почта, мультимедийное образование и др.);

— гарантирует свободу слова независимо от технологической среды распространения информации;

— принимает меры по укреплению многонациональной культуры, русского и национальных языков, противостоит информационно-культурной экспансии других стран, осуществляемой через СМИ и открытые информсети, способствует сохранению языковой и культурной самобытности, вырабатывает госполитику по развитию российской части Интернета;

— обеспечивает широкое использование телемедицины для населения отдаленных регионов;

— осуществляет и целенаправленное использование ИКТ для расширения диалога власти и граждан.

Государство обеспечивает доступ к общественной информации. Информация должна быть открыта для всех и предоставляться с гарантией достоверности и полноты. Основная, первичная информация предоставляется населению бесплатно.

Нельзя не отвечать на новые вызовы международной, национальной, общественной и личной безопасности при движении к инфообществу.

Необходимо смещение центра тяжести процессов перехода к инфообществу из столицы на периферию, широкое привлечение региональных и муниципальных органов власти к участию в процессах информатизации по всем направлениям.

Переход к инфообществу требует широкой психологической и пропагандистской поддержки в общественном мнении.

Создание развитой среды инфообщества, рассматриваемой как совокупность технико-технологических, социально-политических, экономических и социально-культурных компонентов, факторов и условий, при которых информация и знания становятся реальным ресурсом социально-экономического и духовного развития России.

К особенностям перехода России к инфообществу были отнесены:

- нестабильность политического и экономического положения в стране, не позволяющая государству быстро и эффективно решать проблемы обеспечения перехода к инфообществу, рассчитанного на перспективу;
- возрастающий уровень регионализации страны, снижение уровня и возможностей централизованного управления, возрастание степени воздействия, в том числе и финансового, местных органов власти на ход процессов информатизации;
- экономические условия, характерные для переходной экономики: отсутствие свободных инвестиций для финансирования программ и проектов, реализующих стратегию перехода к инфообществу, существенное падение объемов производства и прежде всего в высокотехнологичных отраслях, общий застой в экономической деятельности и значительное снижение уровня жизни населения;
- снижение потребности в информации в госсекторе экономики и рост информационных потребностей населения и общества в целом в политической, экономической и социальной информации;
- недостаточно высокий уровень развития инфраструктуры ИКТ и промышленного производства информационных средств, продуктов и услуг, отсутствие средств для их модернизации и расширения;
- вялое проведение рыночных реформ в экономики страны в целом и динамичное развитие российского рынка ИКТ, продуктов и услуг;
- высокий уровень монополизации СМИ, слабая подконтрольность обществу системы формирования общественного сознания;
- опережающее создание различных систем связи — каналы

передачи информации, коммутирующие комплексы, средства связи и т.д. — и индустрии предоставления информационных услуг;

- наличие высокого научного, образовательного и культурного потенциала, созданного в СССР и еще сохраняющегося в России;
- сравнительно дешевая интеллектуальная рабочая сила, еще способная ставить и решать сложные научно-технические проблемы, движущей силой которой в большой степени является энтузиазм.

Авторы концепции считают, что Россия не может быть исключением и возможны два варианта перехода к инфообществу.

Первый вариант — повторение того пути, который уже пройден или проходится другими странами, в основном европейскими. Он требует значительных капиталовложений, достаточно короткий по времени (не более 7–10 лет до выхода на среднеевропейский уровень информатизации при условии 2–3% темпа экономического роста). Движение по этому варианту будет обеспечиваться средствами (не менее 5–7% ВВП). Кроме того, этот путь будет требовать существенного изменения российского менталитета и переориентации общественного сознания на цели, приоритеты и направления развития, свойственные американскому или европейскому образу жизни.

Второй вариант — нахождение пути, ориентированного на чисто российские критерии и характеристики качества жизни, социально-культурные особенности и требующего в сегодняшних социально-экономических условиях лишь минимальных капиталовложений со стороны государства. Этот путь нетрадиционный, неапробированный. Однако он требует хотя бы минимальных темпов экономического роста, политической стабильности в обществе и политической воли исполнительной и законодательной власти, поставившей перед обществом задачу перехода к инфообществу.

Для реализации первого пути требуется получить основные объемы инвестиций из зарубежных источников или от отечественных коммерческих структур и населения. Авторы концепции справедливо считают, что данный вариант в условиях 1999 г. был не реальным. Основой российского пути было определено следующее:

- информатизация всей системы общего и специального образования — от детского сада до высшей школы и последующих форм переподготовки специалистов;
- повышение роли квалификации, профессионализма и способностей к творчеству как важнейших характеристик человеческого потенциала;

- формирование и развитие индустрии ИКТ и услуг, в т.ч. домашней компьютеризации, ориентированной на массового потребителя;
- обеспечение сферы информационных услуг духовным содержанием, отвечающим российским культурно-историческим традициям, в том числе организация мощного русскоязычного сектора в Интернете.

В концепции отмечается, что Россия может выступить как носитель специфической модели цивилизационного развития, во многом корректирующей западный эталон. Историческая преемственность, национальная идентичность, восстановление нравственного сознания, образование единого духовного пространства страны — таковы основные особенности выбираемого пути России к инфообществу.

Насыщение сферы информуслуг духовным содержанием, отвечающим российским культурно-историческим традициям, является **политической** задачей, решение которой должно обеспечить передачу новому поколению всего многообразия российской культуры, воспитания этого поколения в атмосфере национальных духовных ценностей и идеалов, максимально уменьшить негативное воздействие на молодых людей англоязычной информационной экспансии, культурно-оккупационного характера Интернета. Должна быть оказана всесторонняя поддержка организации мощного русскоязычного сектора в Интернете. Все это создаст предпосылки для преодоления идеологического диктата и распространения политического и духовного влияния США через современные коммуникационные сети и системы.

Основные направления реализации предлагаемого в концепции пути перехода в инфообщество охватывают две главные составляющие:

- создание и развитие технико-технологической базы реализации выбранного пути;
- разработку и реализацию политических, социальных, экономических, правовых, организационных и культурных решений.

Оба эти направления рассматривались в качестве основных объектов госполитики обеспечения перехода к инфообществу. Эти направления выбираются на основе определения приоритетов и временных горизонтов развития входящих в них элементов, учета тенденций их эволюции в развитых странах, оценки исходного положения.

В Концепции особо подчеркивается, что ведущая роль в развитии инфообщества должна принадлежать государству. В связи с этим его первоочередная задача заключается в развитии соответствующей

законодательной базы. Правовые основы формирования инфообщества в России закреплены рядом федеральных законов: «Об информации, информатизации и защите информации», «О связи», «Об участии в международном информационном обмене», «О средствах массовой информации», «О государственной тайне», «Об авторском праве и смежных правах», «О правовой охране программ для ЭВМ и баз данных» и др.

Однако, несмотря на такое количество регламентирующих документов, еще не все вопросы, требующие правового регулирования в связи с формированием инфообщества в России и интеграцией ее в глобальное информационное пространство, имеют должное решение. В частности, интенсивное развитие Интернета в России требует совершенствования законодательства, регулирующего отношения субъектов при использовании сети. Особого внимания заслуживает правовое регулирование электронной коммерции. Можно сказать, что правовая основа становления инфообщества только начинает создаваться в стране и может быть качественно сформирована, как представляется, только при условии системного ее развития и завершения на региональном уровне.

Данная проблематика подробнее рассматривается в следующих параграфах.

4.2. Суть федеральной целевой программы «Электронная Россия»

В изложении ФЦП «Электронная Россия на 2002–2010 гг.», как правило, превалируют два подхода: либо полное изложение, либо достаточно ее краткое описание. Предлагаемый вариант – это попытка найти нечто среднее – максимум ее положений при минимизации ее объема в увязке с другими важными концептуальными документами отрасли.

4.2.1. Содержание проблемы и обоснование необходимости ее решения

Идея разработки ФЦП «Электронная Россия на 2002–2010 гг.» возникла в 2000 г., когда в ходе работы МЭРТ России над стратегическим планом развития страны до 2010 г. стало понятно, что для сокращения отставания от развитых стран, необходимо резко ускорить развитие сектора ИКТ.

В феврале 2001 г. правительством было издано распоряжение о разработке данной программы. После многочисленных согласований, выяснения мнения делового сообщества и внесения соответствующих корректив, как в содержательную часть программы, так и в ее бюджет, в январе 2002 г. «Электронная Россия» была одобрена правительством. Координатором ФЦП было утверждено Минсвязи.

В ФЦП отмечено[3], что, несмотря на высокие темпы развития ИКТ в последнее десятилетие, Россия не смогла сократить отставание от промышленно развитых стран в уровне информатизации экономики и общества. Отчасти такое положение вызвано общеэкономическими причинами (длительный кризис в экономике, низкий уровень материального благосостояния большинства населения). Вместе с тем недостаточное развитие ИКТ в России усугубляется целым рядом факторов, создающих препятствия для широкого внедрения и использования ИКТ в экономике, развития производства в сфере ИКТ:

- несовершенная нормативная правовая база, разрабатывавшаяся без учета возможностей современных ИКТ;
- недостаточное развитие ИКТ в области госуправления, неготовность органов власти к применению технологий управления и организации взаимодействия с гражданами и хозяйствующими субъектами;
- отсутствие целостной информационной инфраструктуры и эффективной информационной поддержки рынков товаров и услуг, в том числе в сфере электронной торговли;
- недостаточный уровень подготовки кадров в области создания и использования ИКТ;
- барьеры, возникающие из-за недостатков в регулировании экономической деятельности при выходе российских предприятий и других организаций сферы ИКТ на российский и мировой рынки;
- высокий уровень монополизации сетей связи, создающий барьеры для их использования и приводящий к перекосам в тарифной политике.

Процессы информатизации уже активно идут на всех уровнях, многие мероприятия, направленные на развитие ИКТ, реализуются в рамках федеральных, региональных и ведомственных программ.

ФЦП должна обеспечить формирование нормативной правовой базы в сфере ИКТ, развитие ИКТ инфраструктуры, сформировать условия для подключения к открытым информсистемам (в т.ч. посредством Интернета), а также обеспечить эффективное взаимодей-

[3] http://www.minsvyaz.ru/site.shtml?id=1100

ствие органов госвласти и органов МСУ с гражданами и хозяйствующими субъектами на основе широкого внедрения ИКТ. В процессе выполнения Программы уточняются общие направления развития ИКТ (основные принципы, стандарты и типовые решения по реализации проектов) как одного из основных направлений социально-экономического развития страны.

4.2.2.Цели, задачи и сроки реализации

Основными целями Программы являются создание условий для развития демократии, повышение эффективности функционирования экономики, госуправления и местного самоуправления (МСУ) за счет внедрения и массового распространения ИКТ, обеспечения прав на свободный поиск, получение, передачу, производство и распространение информации, расширения подготовки специалистов по ИКТ и квалифицированных пользователей.

Реализация Программы позволит:

- эффективно использовать интеллектуальный и кадровый потенциал России в сфере ИКТ;
- обеспечить гармоничное вхождение России в мировую экономику на основе кооперации и информационной открытости;
- преодолеть отставание России от развитых стран в уровне использования и развития ИКТ;
- обеспечить равноправное вхождение граждан России в ГИО на основе соблюдения прав человека, в том числе права на свободный поиск, получение, передачу, производство и распространение информации, а также права на обеспечение конфиденциальности любой охраняемой законом информации, имеющейся в информсистемах.

Для достижения целей ФЦП необходимо решить следующие задачи:

- сформировать эффективную нормативную правовую базу в сфере ИКТ, регулирующую в том числе вопросы обеспечения информационной безопасности и реализации конституционных прав;
- повысить эффективность взаимодействия органов госвласти и органов МСУ как между собой, так и с хозяйствующими субъектами и гражданами на основе использования современных ИКТ;
- обеспечить условия для повышения эффективности и более широкого использования ИКТ в экономической и социальной сфере;
- повысить уровень подготовки и переподготовки кадров за счет совершенствования образования на базе ИКТ;

- содействовать развитию независимых СМИ посредством стимулирования внедрения ИКТ в их деятельность;
- содействовать развитию инфраструктуры ИКТ и возможностей подключения к открытым информсистемам для граждан и хозяйствующих субъектов, а также существенно повысить качество предоставляемых услуг в этой области;
- сформировать единую инфраструктуру ИКТ, необходимую для совершенствования работы органов госвласти и органов МСУ, предприятий и других организаций;
- сформировать условия, необходимые для широкого использования на товарных рынках России механизмов электронной торговли, способствующих ускорению продвижения товаров (услуг), поддержанию стабильного воспроизводства, удовлетворению нужд потребителей и повышению эффективности управления поставками продукции для федеральных госнужд.

Цели и задачи Программы определены с учетом Стратегии социально-экономического развития России на период до 2010 г., основных положений Окинавской хартии ГИО, Концепции формирования и развития единого информпространства и соответствующих государственных информресурсов, Доктрины информационной безопасности России.

4.2.3. Три этапа Программы

На **первом** этапе (2002 г.) формируются предпосылки для реализации мероприятий Программы. Это предполагает проведение анализа нормативной правовой базы с целью выявления ключевых проблем, препятствующих широкому внедрению ИКТ, изучение уровня информатизации экономики, анализ эффективности расходования бюджетных средств, выделяемых на информатизацию, проведение полного учета госинформресурсов, анализ зарубежного опыта реализации подобных программ, изучение опыта работы в сфере ИКТ различных организаций.

Формируются системы мониторинга:

- мировых тенденций развития ИКТ и их использования в социально-экономической сфере;
- уровня распространения ИКТ в стране;
- эффективности расходования бюджетных средств в сфере информатизации;
- эффективности использования ИКТ, информресурсов в органах госвласти и бюджетных организациях, обеспеченности их техническими средствами обработки информации и средствами связи;

• эффективности действующей нормативной правовой базы по использованию ИКТ, в том числе в социально-экономической сфере.

На первом этапе готовится также пакет законопроектов, направленных на решение проблем, связанных с созданием и распространением электронных документов, развитием электронной торговли, снижением административных барьеров, препятствующих выходу российских организаций на рынки ИКТ, гармонизацией законодательства России в сфере ИКТ с положениями международных конвенций и законодательством ЕС.

Реализуются опытные проекты по переходу к электронному документообороту (ЭДО) в органах госвласти и органах МСУ, развитию инфраструктуры ИКТ и подключению к компьютерным сетям органов госвласти, органов МСУ и бюджетных организаций, развитию системы электронной торговли и поддержки рынка товаров (услуг), развитию системы подготовки специалистов для сферы ИКТ и пользователей. Осуществление опытных проектов по подключению к компьютерным сетям органов госвласти, органов МСУ и бюджетных организаций, созданию общественных пунктов подключения к общедоступным информсистемам.

На **втором** этапе (2003–2004 гг.) реализуются проекты, обеспечивающие взаимодействие органов госвласти и органов МСУ с гражданами и хозяйствующими субъектами в сфере налогообложения, по вопросам оформления таможенной документации, регистрации и ликвидации юридических лиц, выдачи лицензий и сертификатов, подготовки и представления отчетной документации, предусмотренной законодательством, об акционерных обществах, рынке ценных бумаг и поставках продукции для госнужд.

Реализуется комплекс мероприятий по внедрению ИКТ в организациях госсектора экономики с целью создания системы мониторинга их финансово-экономической деятельности, реализации опытных проектов по внедрению унифицированных информсистем для предприятий оборонно-промышленного комплекса. Создаются предпосылки для обеспечения передачи находящихся в госсобственности передовых ИКТ организациям гражданской сферы, а также организуются технопарки как центры развития инновационного предпринимательства в сфере ИКТ.

Создается основа единой инфраструктуры ИКТ для органов госвласти и органов МСУ, бюджетных и некоммерческих организаций, системы электронной торговли в сфере поставок продукции для федеральных госнужд и для общественных пунктов подключения к информсистемам.

Формируется современная материально-техническая база для подготовки в ведущих образовательных учреждениях страны специалистов в сфере ИКТ и увеличено число их выпускников. Продолжается совершенствование нормативной правовой базы в сфере ИКТ. Развертывается деятельность по продвижению российских товаров и услуг в сфере ИКТ на мировом рынке.

На **третьем** этапе (2005–2010 гг.) создаются предпосылки для распространения ИКТ во всех сферах на основе единой инфраструктуры ИКТ и использования системы электронной торговли.

Обеспечивается комплексное внедрение системы электронной торговли в сфере поставок продукции для госнужд на федеральном уровне и уровне субъектов Федерации, стандартизованного ЭДО и систем обеспечения информбезопасности.

Завершается формирование инфраструктуры ИКТ для органов госвласти и органов МСУ, бюджетных и некоммерческих организаций, общественных пунктов подключения к общедоступным информсистемам.

В результате создания эффективной системы правового регулирования, функционирования единой инфраструктуры ИКТ, совершенствования системы госуправления и подготовки кадров в сфере ИКТ формируются предпосылки для структурной перестройки экономики.

4.2.4. Система программных мероприятий

В ФЦП предусматривается реализация мероприятий по следующим основным направлениям.

Совершенствование законодательства и системы госрегулирования в сфере ИКТ:

- создание правовой базы для решения проблем, связанных с производством и распространением документов в электронной форме, снижением административных барьеров и ограничений, препятствующих выходу организаций России на рынки ИКТ;
- обеспечение равных прав на получение информации из всех общедоступных информсистем;
- усиление контроля целесообразности расширения требований к хозяйствующим субъектам со стороны госорганов и МСУ;
- применение средств криптографии в сфере гражданско-правовых отношений.

Правовое регулирование ИКТ основывается на следующих принципах:

- обеспечение единства информпространства на территории

России, ликвидация региональных и ведомственных барьеров на пути распространения информации;

- обеспечение беспрепятственной интеграции России в международные системы информобмена;
- обеспечение права каждого на свободное получение информации из общедоступных информсистем;
- гласность и открытость разработки регулирующих норм путем привлечения общественности и предпринимателей к подготовке и обсуждению их проектов;
- гласность и открытость при рассмотрении заявлений на получение лицензий и сертификатов, общественный контроль за обоснованностью их выдачи или отказа в выдаче;
- создание равных условий и устранение монополизма в сфере ИКТ;
- создание правовых условий для использования ЭДО в госуправлении и гражданско-правовой сфере;
- правовое решение проблем, связанных с проведением оперативно-розыскной деятельности в компьютерных сетях;
- упрощение процедур экспорта высокотехнологичной продукции, производимой в сфере ИКТ;
- комплексный подход к совершенствованию законодательства России в сфере ИКТ и его гармонизация с положениями международных конвенций и законодательством государств — членов ЕС.

Обеспечение открытости в деятельности органов госвласти и общедоступности госинформресурсов, создание условий для взаимодействия между органами госвласти и гражданами на основе использования ИКТ. Основными задачами этого направления являются расширение объема информации и перечня информуслуг, предоставляемых гражданам и хозяйствующим субъектам органами госвласти и органами МСУ, формирование механизма общественного контроля их деятельности.

Решение этих задач будет основано на следующих принципах:

- открытость деятельности органов госвласти и общедоступность госинформресурсов;
- обеспечение оперативного информационного взаимодействия граждан и органов госвласти, повышение доверия граждан к государству;
- открытость процедур, связанных с проведением конкурсов на размещение заказов на поставки товаров, выполнение работ и оказание услуг для федеральных государственных нужд.

Использование ИКТ в работе органов госвласти расширяет объем открытой информации о деятельности этих органов и обеспечивает

гражданам возможность ее оперативного получения из информсистем, в том числе по таким важным вопросам, как законопроектная деятельность, бюджетный процесс, закупки продукции для федеральных госнужд, управление госсобственностью, конкурсное замещение вакантных должностей.

Совершенствование деятельности органов госвласти и органов МСУ на основе использования ИКТ. Повышение эффективности работы органов госвласти и органов МСУ путем обеспечения совместимости стандартов хранения информации и документооборота, подключения к компьютерным сетям органов госвласти и органов МСУ, бюджетных учреждений, реализации отраслевых программ информатизации, создания межведомственных и местных информсистем и баз данных.

Использование ИКТ в деятельности органов госвласти и органов МСУ осуществляется по следующим направлениям:

- развитие системы ЭДО, локальных информационных сетей, использование стандартов делопроизводства и документооборота;
- преимущественное использование алгоритмов и программ для ЭВМ, тексты которых открыты и общедоступны;
- развитие систем межведомственного ЭДО, обеспечивающих сокращение сроков обработки документов;
- повышение качества принимаемых управленческих решений путем распространения опыта, накопленного в социально-экономической сфере, консультирования и повышения квалификации.

Реализация работ сопровождается комплексом оргмероприятий, обеспечивающих координацию деятельности органов власти в сфере информатизации, разработку и внедрение стандартных решений, эффективное использование выделяемых на эти цели бюджетных средств.

Совершенствование взаимодействия органов госвласти и органов МСУ с хозяйствующими субъектами и внедрение ИКТ в экономику.

Для достижения данной задачи предусмотрено:

- обеспечить согласованность действий органов госвласти и органов МСУ в процессе информационного обмена;
- обеспечить совместимость стандартов обмена информацией, документооборота, защиты информации, использования ЭЦП;
- определить последовательность перехода к ЭДО.

В сфере содействия внедрению ИКТ в реальный сектор экономики основными задачами являются:

- развитие рынка научно-технической продукции;

- обеспечение эффективной передачи ИКТ, находящихся в госсобственности, организациям гражданского сектора экономики;
- развитие инфраструктуры ИКТ и создание общественных пунктов подключения к открытым информсистемам;
- сокращение издержек для выхода на рынок ИКТ новых хозяйствующих субъектов и стимулирование их выхода — на мировой рынок ИКТ;
- стимулирование хозяйствующих субъектов к открытости деятельности.

Важная роль в реализации данного направления отводится технопаркам — как центрам развития инновационного предпринимательства в сфере ИКТ.

В рамках данного направления предполагается разработка и реализация комплекса мер по содействию внешнеэкономической деятельности, включающего финансирование части издержек российских предпринимателей в сфере ИКТ при выходе на мировые рынки, содействие продвижению продукции российских предприятий и других организаций на эти рынки, проведение мероприятий, популяризирующих Россию как поставщика продукции и услуг в сфере ИКТ, участие России в международных мероприятиях и программах развития ИКТ и стандартизации в сфере ИКТ, поддержка проведения конференций, симпозиумов, семинаров и других мероприятий по развитию сферы ИКТ.

Развитие системы подготовки специалистов по ИКТ и квалифицированных пользователей. Мероприятия этого направления разработаны с учетом ФЦП «Развитие единой образовательной информационной среды (2001–2005 годы)».

Основными задачами данного направления являются:

- создание в отобранных учреждениях высшего профобразования современной методической и материально-технической базы подготовки и переподготовки специалистов для сферы ИКТ;
- формирование необходимой кадровой, методической и материально-технической базы в образовательных учреждениях начального и среднего профобразования;
- создание нормативной правовой базы информатизации образования и развития системы дистанционного обучения;
- развитие инфраструктуры ИКТ в учреждениях среднего и высшего профобразования;
- развитие системы приема на работу и продвижения по службе на конкурсной основе с использованием ИКТ.

Содействие развитию независимых СМИ посредством внедрения ИКТ:

- обучения работников СМИ методам работы со средствами ИКТ;
- обеспечения общедоступности российских и международных открытых информационных ресурсов с помощью сети Интернет;
- создания электронных версий СМИ и архивов в Интернете.

При принятии решений о выделении средств из бюджета для реализации подобных проектов будут учитываться: профуровень коллективов, наличие обоснованного проекта использования ИКТ и участие редакции в финансировании проекта. Конкурсы проектов проводятся на федеральном и региональном уровнях.

Развитие инфраструктуры ИКТ и создание пунктов подключения к открытым информсистемам. Одна из принципиальных проблем — отсутствие в ряде районов России необходимой инфраструктуры и высокие тарифы на подключение к компьютерным сетям (в т.ч. к сети Интернет). Это делает открытые информсистемы недоступными для граждан с невысокими доходами, а также ограничивает возможность их использования образовательными и научными учреждениями, учреждениями здравоохранения и культуры, бюджетными организациями, местными СМИ, органами госвласти и органами МСУ.

Для решения этих задач предусмотрены следующие мероприятия:

- содействие развитию общей телекоммуникационной инфраструктуры;
- создание пунктов подключения к общедоступным информсистемам.

Реализация первого направления обеспечивается путем снижения административных барьеров и снятия ограничений для предпринимательской деятельности, повышения конкуренции и создания благоприятных условий для притока иностранных инвестиций в сферу ИКТ.

Второе направление осуществляется путем финансирования из бюджета развития пунктов подключения к общедоступным информсистемам органов госвласти, бюджетных и некоммерческих организаций.

За счет средств бюджета предполагается финансировать подключение к компьютерным сетям и текущие расходы на их использование территориальными органами и подразделениями федеральных органов и госучреждений. На условиях долевого финансирования предусматривается реализовать проекты по подключению к компьютерным сетям и оплате текущих расходов госучреждений субъектов Федерации и муниципальных учреждений, образовательных и научных учреждений, учреждений здравоохранения и культуры, местных СМИ, обществен-

ных пунктов подключения к сетям, а также технопарков, создаваемых при университетах и научно-производственных центрах.

Для обеспечения подключения к открытым информсистемам максимально использовать действующую инфраструктуру телекоммуникационных сетей, в том числе сеть связи общего пользования, ведомственные, а также сети, созданные в системе образования и науки.

Разработка и **создание системы электронной торговли**, в т.ч. для осуществления закупок продукции для госнужд. Такая система существенно повысит эффективность использования средств федерального бюджета и бюджетов субъектов Федерации при осуществлении госзакупок, а также создаст предпосылки для широкого использования ИКТ в процессе взаимодействия органов госвласти и хозяйствующих субъектов.

Для достижения этих целей необходимо создать:

- единую инфраструктуру электронной торговли, состоящую из информационно-маркетинговых центров (ИМЦ);
- систему электронной торговли для осуществления закупок продукции для федеральных государственных нужд;
- единую базу данных товаров и услуг и систему ее поддержки.

Создание системы электронной торговли для осуществления закупок продукции для федеральных госнужд позволит автоматизировать эти процессы в федеральных органах исполнительной власти, значительно уменьшить издержки госзаказчиков при проведении конкурсов, сократить потери и злоупотребления. При этом для госзаказчиков создаются типовые комплексы аппаратных и программных средств для проведения электронной торговли при осуществлении закупок продукции для госнужд. Ожидается, что экономия бюджетных средств после внедрения системы составит 15%.

Система ИМЦ создается для решения следующих задач:

- формирование единого информпространства, объединяющего данные о предложении и спросе по всей номенклатуре товаров и услуг;
- подготовка информационно-аналитических материалов по различным аспектам предложения и спроса товаров и услуг в регионах и в стране;
- формирование условий для значительного увеличения числа хозяйствующих субъектов — постоянных пользователей в ЛВС;
- обеспечение информационной и функциональной взаимосвязи всех элементов, входящих в систему электронной торговли.

Создание системы ИМЦ будет способствовать поддержке и актуализации разрабатываемой единой базы данных о продукции и услу-

гах, которая через компьютерные сети будет доступна для всех граждан, хозяйствующих субъектов и органов госвласти.

Формирование общественной поддержки выполнения мероприятий:

- организация научно-практических конференций по развитию ИКТ и их использованию в экономике и социально-экономической сфере;
- реализация системы мониторинга эффективности использования ИКТ и информресурсов в органах госвласти и госсекторе экономики, а также технической обеспеченности органов госвласти;
- внедрение системы для слежения за выполнением нормативных правовых документов в области ИКТ, для выявления их нарушений, демонополизации и снижения административных барьеров;
- организация обсуждения через Интернет стандартов, необходимых для распространения ИКТ, анализ распространения стандартов ИКТ и их применения в деятельности независимых организаций, что даст возможность вырабатывать стандарты по ИКТ, сочетающие международную совместимость программных и технических средств с интересами государства, граждан и хозяйствующих субъектов;
- обеспечение широкого информсопровождения ФЦП для привлечения к ней общественного внимания, осуществления поддержки ее реализации со стороны органов госвласти и органов МСУ, предпринимательских кругов, организаций в сфере науки, культуры и образования. В Интернете создается страница о реализации ФЦП[4];
- осуществление мониторинга и анализ освещения в СМИ мероприятий, проводимых в рамках ФЦП, публикация аналитических обзоров о ее реализации, отражающих реакцию на нее СМИ;
- ежегодное проведение конкурсов «Лучшее высшее учебное заведение в сфере ИКТ», «Лучшая школа в сфере ИКТ», «Лучший регион в сфере ИКТ», «Лучшее государственное учреждение в сфере ИКТ» для стимулирования внедрения и развития ИКТ.

4.2.5. Ресурсное обеспечение, управление и контроль реализации

Общий объем финансовых ресурсов, необходимых для реализации Программы, составляет 77 179,1 млн рублей (в ценах 2002 г.), в т.ч. средства федерального бюджета — 39 383 млн рублей, субъектов Федерации — 22 610,1 млн рублей, внебюджетные источники — 15 186 млн рублей.

Объем финансирования реализации первого этапа Программы

[4] http://www.e-rus.ru/main.shtml

(2002 г.) — 2604,4 млн рублей, второго этапа (2003–2004 гг.) — 25 480,5 млн рублей, третьего этапа (2005–2010 гг.) — 49 094,2 млн рублей.

Для второго этапа Программы из федерального бюджета выделяется 13 973,8 млн рублей (или 54,8%). Из средств бюджетов субъектов Федерации и местных бюджетов выделяется 7501,9 млн рублей (или 29,4%) и из внебюджетных источников — 4004,8 млн рублей (или 15,7%). Инвестиции составят 7987,6 млн рублей (или 57,2%), расходы на НИОКР — 1327,6 млн рублей (или 9,5%) и на прочие нужды — 4658,6 млн рублей (или 33,3%).

Для третьего этапа ФЦП из федерального бюджета планировалось выделить 25059,3 млн. рублей (51% объема финансирования). Из средств бюджетов субъектов РФ и местных бюджетов — 13 848,5 млн рублей (или 28,2%) и из внебюджетных источников — 10 186,4 млн рублей (или 20,7%). На третьем этапе инвестиции составят 13 380,3 млн рублей (или 53,4%), расходы на НИОКР — 1765,5 млн рублей (или 7%) и на прочие нужды — 9913,45 млн рублей (или 39,6%).

Мининформсвязи России совместно с другими госзаказчиками разрабатывает и направляет в Минфин России сводную заявку на финансирование мероприятий Программы за счет средств бюджета на очередной год, а затем, с учетом средств, выделяемых на реализацию Программы из всех источников, и предварительных результатов выполнения мероприятий Программы, уточняет мероприятия, промежуточные сроки реализации и объемы их финансирования.

Выполнение мероприятий осуществляется посредством заключения госконтрактов между госзаказчиками и исполнителями программных мероприятий. Организации для выполнения мероприятий определяются в соответствии с Федеральным законом «О конкурсах на размещение заказов на поставки товаров, выполнение работ, оказание услуг для государственных нужд». В объемы финансирования мероприятий Программы включены расходы на осуществление конкурсных процедур.

Одним из принципов ФЦП является привлечение внебюджетных финансовых средств для выполнения тех мероприятий, которые могут иметь коммерческую направленность. Также привлекаются средства субъектов Федерации и местных бюджетов, средства МБРР, российских и иностранных инвесторов, других организаций. Формы их участия определяются договорами между ними и госзаказчиками ФЦП. Средства федерального бюджета для реализации ФЦП, представляющих интерес для регионов, отраслей и

ведомств, предоставляются на условиях долевого финансирования целевых расходов.

Для управления ФЦП Минсвязи создало дирекцию и совместно с другими госзаказчиками разрабатывает и направляет в Минфин сводную заявку на финансирование мероприятий за счет бюджета на очередной год, ежегодно докладывает о ходе реализации Программы до 1 марта в МЭРТ (по инвестициям) и в Минфин России (по расходованию средств бюджета).

Для координации реализации ФЦП и координации вопросов финансирования других федеральных, ведомственных и региональных программ образована межведомственная комиссия (МВК). В ее рамках создан экспертный совет из представителей деловых кругов, вузов, РАН, других научных и профессиональных организаций, Торгово-промышленной палаты, федеральных органов власти и субъектов РФ.

В заключительном разделе ФЦП описываются ожидаемые результаты от ее реализации. Представляется оправданным проанализировать ход выполнения Программы в конце главы совместно с итогами реализации рассматриваемой в следующем параграфе «Концепции использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года» как продолжением ФЦП «Электронная Россия».

4.3. ИКТ и информационная политика России в условиях реформирования государственной службы

ФЦП «Электронная Россия» стала основой для создания ряда новых концепций информационного развития России. Одной их самых актуальных из них стала Концепция развития информсистем в деятельности федеральных органов госвласти, появлению которой предшествовал ряд других важных государственных программ.

4.3.1. Федеральная программа «Реформирование государственной службы Российской Федерации (2003–2005 гг.)»

В целях повышения эффективности государственной службы в интересах укрепления государства и развития гражданского общества Президент России В.В.Путин 15 августа 2001 года подписал Указ «О концепции реформирования системы государственной службы Российской Федерации».

Указом от 19 ноября 2002 г. № 1336 Президентом России была

утверждена Федеральная программа «Реформирование государственной службы Российской Федерации (2003–2005 гг.)».

В указе подчеркнута необходимость осуществить в 2003–2005 гг. комплекс мероприятий, направленных на совершенствование правовых, организационных, финансовых и методических основ государственной службы России.

Среди мероприятий программы имеются и меры, направленные на повышение эффективности государственной службы путем внедрения новейших информационно- коммуникационных технологий.

Важным документом в данном контексте стал Указ Президента Российской Федерации от 23 июля 2003 г. № 824 «О мерах по проведению административной реформы в 2003–2004 годах».

4.3.2. Концепция развития информационных систем в деятельности федеральных органов власти (2004 г.)

Логичным продолжением ФЦП «Электронная Россия» стала «Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года» (одобрена Правительством России 27 сентября 2004 г., рп-1044). Концепция, разработанная Мининформсвязи, определяет основные приоритеты, принципы и направления реализации единой госполитики в сфере использования ИКТ и является конкретным шагом на пути создания **электронного правительства**.

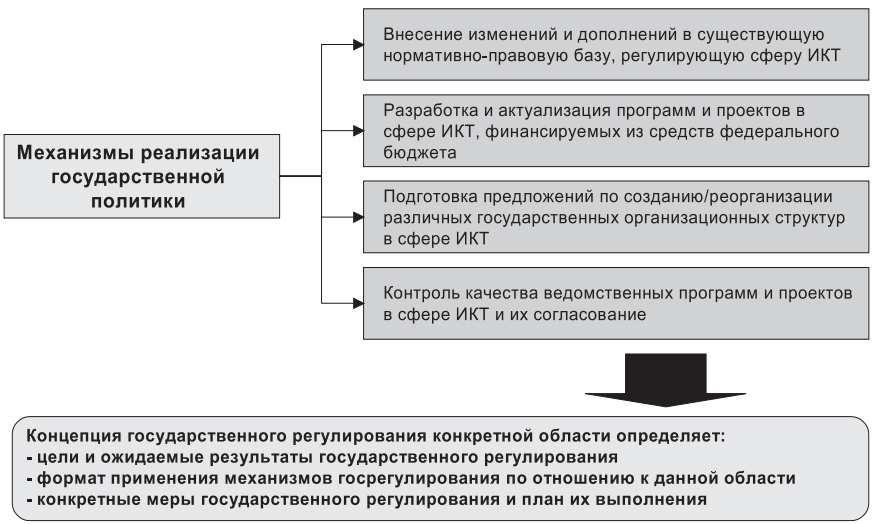
Анализ показывает, что после воссоздания Мининформсвязи в мае 2004 г. оно во многих измерениях позиционируется по-новому и по-иному строится механизм реализации госполитики в сфере ИКТ[5].

[5] www.riocenter.ru/region.ppt

Новое позиционирование Мининформсвязи России

Новый подход можно видеть и в механизме реализации государственной политики в сфере развития и использования ИКТ.

Основные механизмы реализации государственной политики в сфере развития и использования ИКТ



До принятия Концепции информатизации госорганов на федеральном уровне проекты реализовывались в рамках отдельных программ и не были увязаны между собой. Одобренная Концепция определяет основные приоритеты госполитики в сфере использования ИТ в федеральных органах госвласти в соответствии с задачами модернизации госуправления.

Согласно Концепции, основным механизмом реализации единой согласованной госполитики в сфере использования ИКТ в федеральных органах госвласти является ФЦП «Электронная Россия (2002 — 2010 годы)».

Как подчеркнул министр Л.Рейман, утвержденная Концепция — это целевая работа, направленная на более системное, быстрое и эффективное внедрение ИКТ в органах госвласти». Бюджет, затраченный на мероприятия в рамках Концепции, будет больше прописанного в ФЦП «Электронная Россия», за счет средств, которые тратятся на ИКТ ведомствами ($0,8–1,5 млрд в год)[6].

С учетом того, что в настоящее время в разных стадиях находятся несколько концепций развития различных сегментов ИКТ отрасли, представляется оправданным привести их базовые цели и задачи[7].

Цели и задачи концепций

Концепция использования ИТ в деятельности федеральных органов государственной власти	Определение плана и основных направлений создания «электронного правительства», обеспечения взаимоувязанного развития ведомственных информационных систем и повышения эффективности расходования бюджетных средств в этой сфере
Концепция региональной информатизации	Унификация подходов к информатизации регионов, определение общей типовой архитектуры информационной системы, обеспечивающей поддержку эффективного государственного управления на уровне региона и общих требований к ее реализации
Концепция развития российского рынка ИТ	Оценка имеющегося ресурса для обеспечения прорыва в этой области и возможной роли отрасли в решении задач снижения сырьевой зависимости экономики, определение основных препятствий на пути ее развития и основных мер, необходимых для создания режима максимального благоприятствования

[6] http://www.cnews.ru/newtop/index.shtml?2004/10/05/166117

[7] www.riocenter.ru/region.ppt

4.3.2.1. Опыт внедрения информационных систем в органах госвласти

На начало 2005 г. в России наработан достаточно успешный опыт внедрения информсистем в ряде органов госвласти. Однако успешность данных решений определяется локальными задачами. Информсистемы позволили достичь сравнительно высоких показателей в области информационных взаимодействий, оказания услуг населению, автоматизации внутриведомственных процессов.

Вместе с тем анализ, проведенный при подготовке первой редакции Концепции в 2003 г., показал разобщенность информсистем в плане стандартов на функциональность и на технологию. Выбор решений по автоматизации субъективен, диктуется рыночными реалиями, бюджетными реалиями, а также рядом иных случайных факторов. В ряде случаев имелись свои стандарты на обмен и управление информацией по причине отсутствия регламентирующих документов федерального уровня.

Накопленный опыт, включая и негативный, стал ценным источником информации – как по текущему состоянию автоматизации, так и по конкретным проблемам внедрения информсистем в различных ведомствах. В этом контексте представляется оправданным сослаться на результаты анализа внедрения информсистем в госсекторе, приведенные на веб-сайте «Электронной России»[8]. Были исследованы следующие типы взаимодействия:

- Внутриведомственная интеграция информационных систем;
- Межведомственная интеграция на уровне данных;
- Межведомственная интеграция на уровне приложений;
- Автоматизация взаимодействия с населением и бизнесом;
- Предоставление услуг населению и бизнесу в режиме on-line.

В качестве параметров оценки были определены пять — наиболее важных с точки зрения концепции электронного правительства:

- Степень автоматизации процесса оказания госуслуги. В контексте административной реформы оказание услуг (публичных или административных) является основой деятельности органов власти. Поэтому автоматизация процесса оказания услуги, а не отдельных операций является ключевой характеристикой информсистем.
- Степень автоматизации взаимодействия участников процесса оказания услуги (критерий эффективности взаимодействия сторон). В зависимости от типа услуги (публичная, административная) состав

[8] http://www.e-rus.ru/upload/docs/20041208155846.doc

участников различен: взаимодействие органов власти с населением, бизнесом и негосударственными организациями; взаимодействие между госорганами. Как правило, точка взаимодействия является наиболее «узким» местом этого процесса.

- Уровень использования межведомственных информресурсов. Критерий эффективности и упорядоченности структуры обмена данными отражает степень интеграции в межведомственное информпространство (доступ к базам данных и знаний, к общему инструментарию: серверы цифровых подписей федерального уровня, системы контроля данных, финансовых операций и др.)
- Модульность, гибкость архитектуры (критерий возможности масштабирования систем и приведения к единому стандарту).
- Степень соответствия требованиям Единой федеральной архитектуры (ЕФА) электронного правительства (критерий непротиворечия и недублируемости госфункций, осуществляемых в рамках единой системы госполномочий), т.к. эффективное взаимодействие информсистем возможно лишь при условии их соответствия единой функциональной модели.

4.3.2.1.1.Единый центр регистрации юридических лиц МНС России[9]

В соответствии с федеральным законом «О внесении изменений в законодательные акты Российской Федерации в части совершенствования процедур государственной регистрации и постановки на учет юридических лиц и индивидуальных предпринимателей» МНС России с 1 января 2004 г. реализует принцип «одного окна».

Концепция «одного окна» предполагает регистрацию, постановку на учет в налоговые органы и во внебюджетные фонды (Пенсионный фонд, Федеральный фонд обязательного медицинского страхования и Фонд социального страхования), а также присвоение кода Госкомстата на основании однократного предоставления документов.

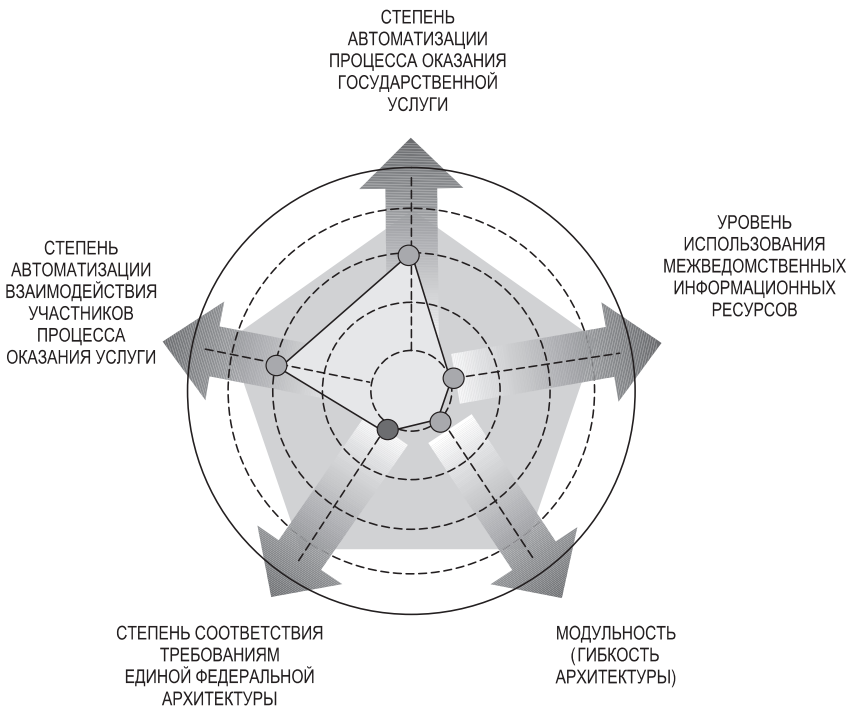
С введением принципа «одного окна» уже на шестой день после подачи документов выдаются свидетельства о регистрации и постановке на налоговый учет. Органы МНС после внесения записи в единый госреестр на шестой день будут передавать информацию об этом в соответствующие внебюджетные фонды и органы статистики.

[9] С мая 2004 г. Федеральная налоговая служба России.

В центре установлен терминал. Клиенту предлагается выбор: подать документы, получить свидетельство, ликвидировать фирму. В ответ терминал выдает талон с номером очереди и зала и предполагаемого время приема. Затем табло приглашает к «одному окну».

В центре работает 51 окно, на обслуживание клиента тратится не более 12 минут. В перспективе — до 7-8 минут. Постановку юридического лица на учет в Пенсионный фонд, Соцстрах и Госкомстат осуществят в течение пяти дней. После этого можно открыть счет в банке и начать свою деятельность.

Оценка системы по ключевым показателям



1. Взаимодействие с клиентом услуги улучшено, однако процесс подготовки документов клиентом никак не автоматизирован.
2. Автоматизация процесса оказания услуги на среднем уровне, т.к. она практически не затрагивает процесс оформления документов.
3. Уровень использования межведомственных ресурсов остался на прежнем уровне.

4. Гибкость архитектуры находится на минимальном уровне, поскольку масштабирование системы не предусмотрено.
5. Требования ЕФА при разработке системы не учитывались.

4.3.2.1.2. Программа «Социальная карточка москвича»

В рамках широкомасштабной программы «Электронная Москва» реализована программа «Социальная карта москвича» – совместная программа Правительства Москвы, Банка Москвы, Московского метрополитена, Комитета социальной защиты населения, Московского городского фонда обязательного медицинского страхования и Московской железной дороги для пенсионеров и других категорий граждан, имеющих социальные льготы. К проекту постоянно подключаются новые участники.

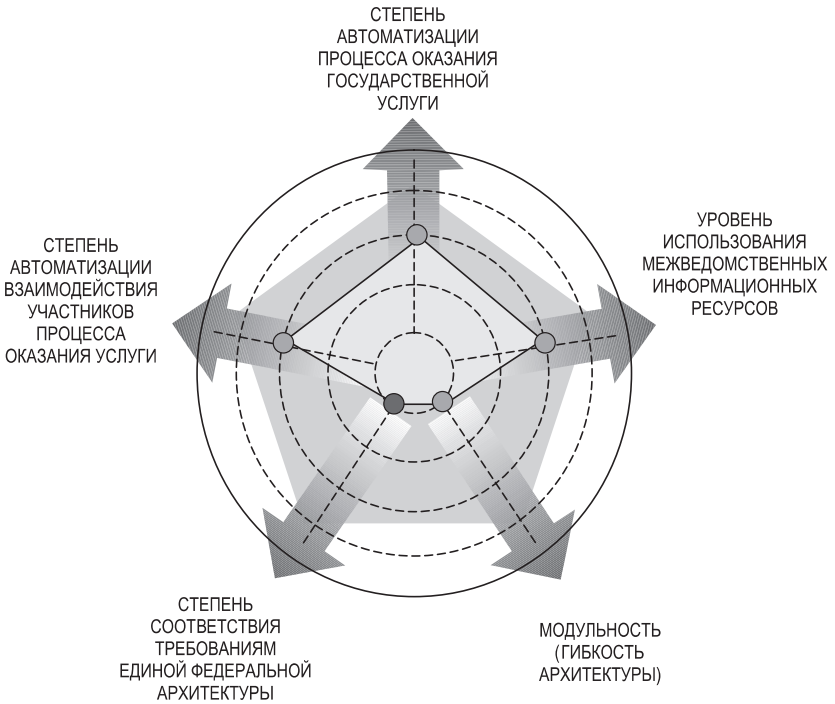
«Социальная карта» совмещает функции расчетной банковской и идентификационной карты и предназначена для обслуживания льготных категорий граждан в предприятиях потребительского рынка и услуг, лечебно-профилактических учреждениях, для обеспечения льготного проезда в метрополитене и на Московской железной дороге. «Социальная карта» фиксирует право льготника на приобретение товаров и услуг по льготным ценам, а также право пользоваться установленными льготами на транспорте.

С 2002 г. введена новая услуга – оплата жилищно-коммунальных услуг (ЖКУ). Основные преимущества услуги:

- услуга позволяет клиентам – держателям «Социальной карты москвича» сэкономить свое время, совершая платежи, не приходя в Банк и не заполняя квитанции об оплате;
- клиент может осуществлять контроль за расходованием своих средств по карте, получая выписку, в которой отражено движение по счету, в любом отделении или банкомате Банка Москвы;
- банк своевременно осуществит оплату ЖКУ и при изменении тарифов сделает перерасчет суммы автоматически.

«Социальная карта» представляет собой пластиковую карту с магнитной полосой и встроенным бесконтактным чипом. Магнитная полоса на карте позволяет получать наличные денежные средства в банкоматах и пунктах выдачи наличных, а также оплачивать товары и услуги в торгово-сервисных предприятиях. Для осуществления расчетов по операциям с использованием «Социальной карты» на имя держателя карты Банком Москвы открывается счет, на который можно переводить денежные средства, в т.ч. предусмотренные программой для льготных категорий граждан.

Оценка системы по ключевым показателям



1. Степень автоматизации оказания услуги довольно высока за счет многофункциональности пластиковых карт (удостоверение личности, финансовые операции, передача данных и др.).

2. Степень автоматизации процесса оказания госуслуги также высока за счет возможности перевода средств (например, социальных пособий, пенсий) на пластиковую карту, а также снятия средств с нее для оплаты ЖКУ и пр.

Под межведомственным информресурсом рассматривается совокупность этих карт, содержащих персональные данные о населении, считываемые локально и используемые для оказания госуслуг.

Вместе с тем:

1. Гибкость архитектуры находится на минимальном уровне, т.к. модернизация пластиковых карт не предусмотрена, существуют ограничения по объему приложений и хранящейся информации.

2. Требования ЕФА при разработке системы не учитывались.

4.3.2.1.3. Информсистемы в Республике Чувашия

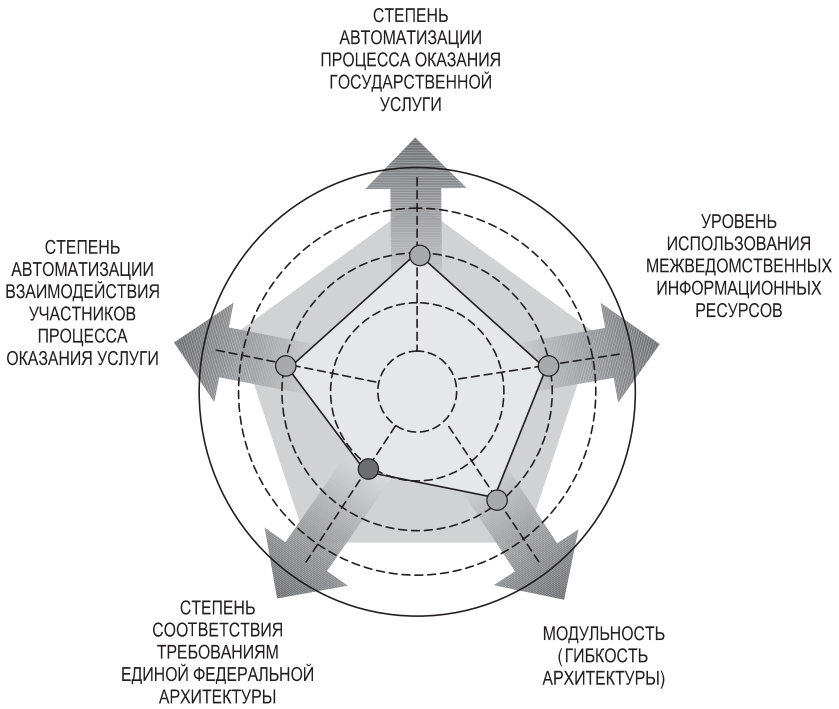
В Чувашии в рамках ФЦП «Электронная Россия» проведены масштабные работы: все муниципальные отделы ЗАГС, районные и городские ОВД, предприятия ЖКХ оснащены компьютерной техникой и подключены к республиканской телекоммуникационной сети. Установлено программное обеспечение, налажен ввод и обмен информацией о движении населения, формируются муниципальные структуры.

В 2004 г. проведена выверка и синхронизация баз данных о населении, поддерживаемых МНС России, Пенсионным фондом, фондом медицинского страхования, ЦИК (ГАС «Выборы») и пр.

Основные цели: обеспечение эффективного автоматизированного информобмена в сфере учета населения, создание информационно-аналитической основы для проведения реформы ЖКХ, улучшение информационного обслуживания населения, сокращение потерь времени при обращении граждан в органы госвласти и МСУ, повышение эффективности использования бюджетных средств на социальные программы, обеспечение адресного предоставления льгот.

Создание информсистемы способствует получению реального экономического эффекта за счет экономии средств пенсионных фондов, фондов медицинского страхования, а также создает основу для усовершенствования системы сбора налогов с физических лиц. Также обеспечивается экономия средств за счет автоматизации социально-демографических обследований и переписи населения, процесса предоставления адресных субсидий, а также унификации системы компенсаций предприятиям ЖКХ.

Оценка системы по ключевым показателям



1. Взаимодействие участников процесса оказания услуг (как публичных, так и административных) автоматизировано.
2. В процессе оказания услуг применяются средства автоматизации доступа к информации, учета и контроля операций.
3. Создано единое информпространство, организована система сбора и централизованного хранения информации. Организовано информационное взаимодействие с органами федерального уровня.
4. Для информационного взаимодействия использованы универсальные стандарты.
5. Соответствие концептуальным положениям архитектуры электронного государства, разрабатываемой в рамках ФЦП «Электронная Россия».

4.3.2.2. Проблемы использования ИКТ в федеральных органах государственной власти

На заседании Правительства России 16 декабря 2004 г. был рассмотрен вопрос «Об использовании современных информационных технологий в деятельности федеральных органов государственной власти». Выставленный на веб-сайт Правительства России пресс-релиз отличается нелицеприятными для отрасли оценками. В нем отмечено, что общие показатели, характеризующие уровень и эффективность использования ИКТ в деятельности федеральных органов госвласти, заметно ухудшились по сравнению с 2003 г. Ожидания, связанные с разработкой и одобрением Правительством России Концепции использования информтехнологий в деятельности федеральных органов госвласти до 2010 г. и намечающимся прорывом в этой сфере, пока не оправдались.

Представленные сведения позволили сделать вывод о фактической консервации сложившейся в 2003 г. ситуации, отсутствии заметного прогресса в решении основных проблем повышения эффективности использования ИКТ в системе госуправления, замедлении общих темпов информатизации и даже ухудшении ранее достигнутых результатов.

Рост объемов бюджетных расходов федеральных органов госвласти на внедрение ИКТ в свою деятельность, обеспечение функционирования и поддержку используемых информсистем сократился примерно на 50% по сравнению с 2003 г. и составил в 2004 г. около 9 млрд рублей. Финансирование задач ведомственной информатизации из средств федерального бюджета — около 7 млрд рублей. До 30% объема выделяемых бюджетных средств на информатизацию федеральных органов госвласти приходится на мероприятия, выполняемые в рамках утвержденных ФЦП.

Доля бюджетных расходов на использование ИКТ в деятельности федеральных органов госвласти в структуре расходов федерального бюджета в 2004 г. сократилась по сравнению с 2003 г. на 5%. Произошло также значительное сокращение бюджетных расходов на обучение работников федеральных органов госвласти навыкам использования ИКТ.

Очевидно, что данная ситуация во многом обусловлена структурной перестройкой в рамках первого этапа административной реформы и привела к приостановке реализации ряда проектов внедрения ИКТ. В силу этого значительная доля реализуемых проектов приходится на федеральные органы госвласти, не претерпевшие значительных изменений в результате административной реформы.

Замедление темпов роста бюджетных расходов на ведомственную информатизацию во многом сдерживалось продолжением в 2004 г. масштабных программ и проектов информатизации, финансирование которых осуществлялось за счет международных займов, доля их расходов выросла в 2004 г. до 20% всех расходов и составила около 2,5 млрд рублей.

Реформирование системы федеральных органов исполнительной власти выявило основные недостатки существующих моделей управления ведомственными информсистемами и ресурсами. В результате изменения системы федеральных органов исполнительной власти подавляющее большинство ранее разработанных ведомственных программ информатизации потеряло свою актуальность и требует полной или частичной корректировки с учетом нового разделения функций.

4.3.2.2.1. Развитие ИКТ инфраструктуры

Уровень обеспечения работников федеральных органов госвласти персональными компьютерами в 2004 г. вырос с 28 до 32%. Однако сохранилась ситуация, требующая дополнительной установки к основному компьютеру, используемому сотрудником для работы в локальной сети ведомства, отдельного компьютера для доступа в сеть Интернет.

Ключевой проблемой на уровне ведомств по-прежнему остается подключение территориальных подразделений к центральному аппарату и обеспечения их электронного взаимодействия между собой. Особенно актуальна это для ведомств, имеющих большое число территориальных подразделений — МВД России, МПР России и др.

Не решена задача защиты инфраструктуры ИКТ, обеспечения межведомственного электронного обмена данными. Основная его доля осуществляется через электронную почту, причем часто с использованием почтовых ящиков на публичных серверах.

Несмотря на принятие Федерального закона «Об электронной цифровой подписи», не решен вопрос об использовании ЭЦП, не определен уполномоченный федеральный орган исполнительной власти, ответственный за создание федерального удостоверяющего центра, а также координацию на межведомственном уровне проектов по созданию госсистемы удостоверяющих центров. На практике это приводит к созданию удостоверяющих центров, не соответствующих требованиям безопасности, а используемые средства в ЭЦП зачастую несовместимы между собой.

4.3.2.2.2. Создание государственных информационных ресурсов

Для обеспечения эффективности госуправления важно создание информресурсов федерального значения, содержащих сведения об объектах госучета. В соответствии с Концепцией эти ресурсы должны совместно формироваться и использоваться федеральными органами госвласти. В 2004 г. автоматизированные системы госучета и формируемые ими информресурсы, необходимые для эффективной реализации основных задач госуправления, на федеральном уровне не получили должного развития.

Не сформирован госрегистр населения (ГРН), который в соответствии с концепцией создания системы персонального учета населения (СПУН)[10] является ее информационным ядром, обеспечивающим возможность взаимодействия различных систем учета населения между собой по обмену персональными данными. В рамках создания ГРН должно быть обеспечено присвоение единого уникального идентификатора всем персональным сведениям, размещаемым в системах учета. Сегодня параллельно существуют 18 ведомственных баз данных, но ни одна не содержит полной информации о населении и не обеспечивает взаимодействия с другими ведомствами. Нередко это приводит к дублированию бюджетных расходов на сбор уже имеющихся в других ведомствах персональных данных, а иногда и несоответствию данных по одному и тому же лицу между собой.

Отдельные составляющие СПУН уже разработаны Мининформсвязи России. В частности, в рамках ФЦП «Электронная Россия (2002–2010 гг.)» был реализован ряд проектов по созданию ГРН, который станет интеграционной основой СПУН. Разработку ГРН ведет ФГУП НИИ «Восход», создавший государственную автоматизированную систему «Выборы».

Планируется, что на создание СПУН потребуется около семи лет, но Минэкономразвития и Мининформсвязи поручено представить Правительству России проекты решений о внесении соответствующих изменений в ФЦП «Электронная Россия (2002-2010 гг.)». В 2005 г. ведутся эксперименты по внедрению ГРН в Москве, Санкт-Петербурге, Московской, Ярославской и Калининградской областях и Ханты-Мансийском автономном округе[11].

---

[10] Концепция создания СПУН одобрена распоряжением Правительства Российской Федерации от 9 июня 2005 г. № 748-р.

[11] http://www.minsvyaz.ru/news.shtml?n_id=2717

В этом контексте необходимо отметить как позитивное создание Минздравом России в 2004 г. единого федерального регистра лиц, имеющих право на получение государственной социальной помощи.

В 2004 г. началась реализация проектов по созданию единого банка, содержащего информацию об авиапассажирах и проданных им билетов.

В 2004 г. в ФМС России создана базовая инфраструктура банка данных по учету иностранных граждан и лиц без гражданства, временно или постоянно пребывающих или проживающих на территории России.

Федеральное агентство кадастра объектов недвижимости ведет работы по созданию и координации функционирования информсистемы ведения государственного земельного кадастра и госучета объектов градостроительной деятельности в рамках двух ФЦП. Развернуты программно-технические комплексы, обеспечивающие реализацию необходимых учетных процедур и внесение в базы данных сведений.

В рамках ФЦП «Электронная Россия (2002–2010 гг.)»:

- осуществляется подключение территориальных органов Роснедвижимости всех субъектов Российской Федерации к телекоммуникационным сетям общего назначения;
- ведется создание единой среды электронного обмена документами и сведениями при формировании, инвентаризации, кадастровой оценке, госучете объектов градостроительной деятельности, госучете земельных участков, госрегистрации прав на недвижимое имущество и сделок с ним, а также налогообложении недвижимого имущества.
- решаются проблемы обеспечения интеграции и взаимодействия систем, используемых в деятельности уполномоченных госорганов и организаций в сфере земельно-имущественных отношений.

На уровне отдельных субъектов Федерации формируются базы данных по учету основных видов природных ресурсов. Проблемой остается низкая частота и качество актуализации информресурсов, а также их интеграция на федеральном, региональном и муниципальном уровнях.

4.3.2.2.3. Использование системы электронного документооборота

Практически все федеральные органы госвласти используют системы электронного документооборота (ЭДО) для ведения централизованного учета и регистрации входящих и исходящих документов, их перевода и хранения в электронном виде, а также учета результатов их исполнения.

При этом лишь часть систем позволяет вести ведомственные электронные архивы, наполнение которых происходит через системы потокового сканирования и ввода бумажных документов, автоматизированной обработки электронной почты, факсимильных документов, а также запросов и обращений, поступающих через ведомственные Интернет-сайты.

Используемые системы позволяют обеспечить прохождение этих документов до структурного подразделения или подведомственной организации, учет и контроль своевременности их рассмотрения и исполнения. При этом только в 10% всех федеральных органов госвласти используемые системы ЭДО охватывают сколько-нибудь значительную долю рабочих мест сотрудников управленческого звена центрального аппарата.

Следует отметить внедрение системы штрих-кодирования документов. Как показала практика, эта технология позволяет значительно повысить эффективность всех процессов работы с документами, полностью исключив влияние человеческого фактора, который раньше приводил к неправильному вводу реквизитов входящих документов, медленной регистрации документов и недостаточному контролю за их исполнением.

В рамках ФЦП «Электронная Россия (2002–2010 гг.)» создается также единый электронный архив Президента России.

4.3.2.2.4. Развитие межведомственного взаимодействия. Предоставление услуг населению и организациям

В рамках ФЦП «Электронная Россия (2002–2010 гг.)» ведется реализация ряда проектов, направленных на обеспечение межведомственного взаимодействия в рамках предоставления госуслуг населению и организациям. Наряду с уже описанным проектом «одного окна» ФНС, создается единая госсистема контроля за вывозом товаров с таможенной территории России.

Целью проекта является сокращение бюджетных потерь, повышение эффективности мероприятий по проверке обоснованности применения налоговой ставки «0 процентов» и налоговых вычетов по НДС при экспорте товаров, ускорение и упрощение процедур, связанных с подтверждением фактического вывоза товаров и транспортных средств с таможенной территории России и возвратом экспортного НДС.

По оценкам экспертов, реализация проекта позволит сократить количество экспортных операций с признаками фиктивного экспор-

та (мошеннические действия экспортера с целью многократного возмещения НДС по факту единственной экспортной операции) на 20%, обеспечить экономию бюджетных средств на сумму 39 млрд руб. и экономию финансовых ресурсов хозяйствующих субъектов за счет сокращения срока вывода средств из оборота — на сумму 25 млрд руб. ежегодно.

В соответствии с постановлением Правительства России федеральные органы исполнительной власти обязаны обеспечить размещение в сети Интернет информации о своей деятельности. Однако на этих сайтах не представлена значительная часть информации справочно-информационного и оперативного характера. Опубликованные сведения по своей полноте, структурированности и организации доступа не обеспечивают информационной открытости деятельности федеральных органов госвласти, организации их информвзаимодействия с населением и организациями (только на половине сайтов эта информация носит полный, подробный и оперативный характер).

Более 30% ведомств на начало 2005 г. не имели действующих Интернет-сайтов. Лишь половина сайтов федеральных органов госвласти дают возможность пользователю оформить и направить вопрос руководителю органа или обратиться непосредственно в конкретные структурные подразделения путем заполнения специальных электронных форм.

Применение информтехнологий требует серьезной подготовки, как госзаказчиков, так и представителей бизнеса. Одномоментное введение в силу норм закона, связанных с электронными технологиями госзакупок без создания должных организационных и материальных условий, способно лишь дискредитировать этот эффективный механизм.

4.3.3. Информсистемы поддержки деятельности федеральных органов госвласти

Внедрение информационно-аналитических систем в развитых странах опирается не только на новейшее специальное программное обеспечение, но и на мощные базы данных. В России применение данных систем стало возможным благодаря внедрению в отдельных ведомствах технологий автоматизированного учета и сбора первичных данных и формированию соответствующих баз данных. Использование данного класса систем приобретает особое значение в связи с разделением функций федеральных органов государственной власти на правоустанавливающие, правоприменительные и контрольно-

надзорные и внедрением ключевых показателей результативности их деятельности по достижению целей и задач социально-экономического развития.

Основой для создания госсистемы мониторинга и прогнозирования основных показателей социально-экономического развития, планирования и контроля деятельности федеральных органов госвласти могут стать базы данных, формируемые Федеральной службой госстатистики, а также средства доступа к ним в рамках реализации проекта «Развитие системы государственной статистики», осуществляемого за счет заемных средств.

В настоящее время завершается этап опытной эксплуатации и приемо-сдаточных испытаний системы. По их завершению будет принято решение о тиражировании созданной системы на все территориальные органы Федеральной службы государственной статистики.

На базе отработанных в рамках текущего проекта подсистем планируется обеспечить поэтапное формирование единой инфраструктуры сбора, обработки и хранения статистических данных в электронном виде и создание интегрированного информационного ресурса Федеральной службы.

4.3.3.1. Классификация средств информационно-аналитической работы

Сфера технологического обеспечения информационно-аналитической работы является выражением тех организационных и методологических принципов, которые заложены в основу информационно-аналитического обеспечения в целом, и может быть введена следующая классификация средств ее автоматизации[12]:

- средства сбора данных;
- средства доставки данных;
- средства хранения данных;
- средства обработки данных;
- средства формирования тезауруса;
- средства согласования тезауруса;
- средства интеграции данных;
- средства анализа данных;
- средства моделирования;
- средства интерпретации результатов;
- средства прогнозирования;

[12] *Курносов Ю.В., Конотопов П.Ю.* Аналитика:методология,технология и организация информационно-аналитической работы. – М.: РУСАКИ, 2004. С. 280.

- средства синтеза целей управления;
- средства отображения данных;
- средства поддержки принятия решений;
- средства доведения управляющих воздействий.

К задачам информационно-аналитического характера относятся[13]:

- описание проблемной ситуации и формулировка проблемы;
- выявление причинно-следственных связей и прогноз развития ситуации;
- формирование вариантов и моделирование последствий управленческих решений;
- коллективное решение управленческих задач при изменяющихся целевых функциях с учетом взаимодействия с внешней средой.

Зарубежный и отечественный опыт показывает, что наилучшим образом данные задачи решаются в ситуационных центрах.

4.3.3.2. Ситуационные (кризисные) центры и интеллектуальные кабинеты руководителя

В условиях стремительного роста информпотоков и ограничения времени для принятия стратегических решений критически важным становится создание для руководителей ведомств и иных структур современной информационной и технологической среды, обеспечивающей эффективную поддержку управленческой деятельности.

Важнейшими элементами этой среды являются Ситуационный (Кризисный) центр (СЦ) и Интеллектуальный кабинет руководителя (ИКР). Понятие СЦ связано с поддержкой принятия управленческих решений в кризисных ситуациях и/или обсуждения и решения многоаспектных политических, экономических и иных проблем. Часто в смысл СЦ вкладывается сам процесс мониторинга развития различных ситуаций.

В зависимости от предметной области название «ситуационного 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 инфор-

[13] См.: *Данчуло А.Н.* Информационно-аналитические технологии и ситуационные центры//Государственная служба. 2004. № 4

мационные, телекоммуникационные, программные и методические средства, обеспечивающие процесс доставки и агрегирования информации, а также процесс ее интеллектуального обсуждения участниками анализа с целью выработки соответствующего решения.

На правительственном сайте США дается следующее определение ситуационной комнате Белого дома (White House Situation Room) – это круглосуточный наблюдательный и сигнальный центр, обеспечивающий президента, помощника по национальной безопасности, членов Совета безопасности текущей разведывательной и открытой информацией для выработки и реализации политики в области национальной безопасности.

Другим известным примером СЦ является центр ФБР, называемый Центром стратегической информации и операций (Strategic Information and Operations Center – SIOC), который играл и играет ключевую роль в расследовании событий 11 сентября 2001 г. Центр обеспечивает не только сбор и агрегирование необходимой информации, но и координацию работы по выделенной проблеме различных министерств и ведомств. В частности, по проблеме 11 сентября Центр взаимодействует с более 500 представителями 32 госагентств. Центр располагается в особо охраняемой зоне здания ФБР. В центр входят две комнаты командования, комната управления и комната конференций. Все помещения оборудованы специальными средствами отображения (большими экранами и мультиэкранными комплексами).

Подобные центры управления и поддержки принятия решений созданы в Пентагоне, других государственных учреждениях (Air Force Innovation Center, Defense Systems Management College, Federal Aviation Administration, Department of State, министерства обороны стран Западной Европы, UK Post Office и многих других). В условиях обострения международной обстановки, в т.ч. в контексте борьбы с терроризмом, СЦ активно создаются во внешнеполитических ведомствах ведущих стран мира.

Из открытых источников известно, что СЦ существуют не только в госструктурах, но и в крупных коммерческих организациях, где есть необходимость оперативного принятия управленческих решений на базе многоаспектной информации. В частности, ситцентры поддержки принятия решений оборудованы в компаниях PriceWaterHouse Coopers, Boeing, Aerospatiale, Nokia, Eastman Chemicals, Computer Science Corporation, Grenridge Insurance (Norway), во многих нефтяных корпорациях.

В России также созданы СЦ у руководства страны, ряда федеральных служб, Минатоме и т.п. В последнее время они создаются в коммерческих структурах — Лукойл, ТНК и т.д.

С технологической точки зрения СЦ и ИКР предприятия (организации, администрации) являются составными частями его информационно-телекоммуникационной системы (ИТКС). При этом используются самые современные ИКТ (Интернет/Интранет порталы, аналитические программы и базы данных, мультимедийные, в т.ч. видео, источники информации, геоинформационные технологии, видеоконференции, эффективные средства отображения и т.п.).

Можно выделить ряд признаков «ситуационности» проблемы, указывающих на целесообразность их решения с помощью информационно-аналитических технологий, поддерживаемых ситуационными центрами:

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

Основные цели создания СЦ и ИКР:

- 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 онлайн с лент мировых агентств, финансовых структур и т.п. с использованием современных средств отображения;
- организация и обеспечение технологической поддержки проведения совещаний, коллегий и т.п. с использованием современных методик коллективной работы, включая методы «мозгового штурма» и т.п., протоколирование проводимых мероприятий;
- обеспечение возможности удаленного подключения и эффективной работы распределенных групп экспертов;
- обеспечение возможности эффективного и оперативного управления руководителем предприятия своими подразделениями, в т. ч., удаленными, путем личного визуального контакта;
- обеспечение непосредственного доступа руководства и специалистов предприятия к достоверной информации из различных источников с выдачей ее на один экран (реализация принципа «единого окна»), улучшение представления отчетной информации;

- повышение оперативности и качества управленческих решений на основе использования аналитических и прогнозных средств;
- совершенствование взаимодействия с ситуационными центрами и аналитическими структурами других предприятий и ведомств.

Из вышесказанного следует, что существует два основных подхода построения ситуационных центров:

- локальный ситуационный центр;
- распределенный ситуационный центр.

Перспективным является построение распределенного СЦ организации. По сути это – совокупность связанных между собой ситцентров, ориентированных на реализацию концепции управления знаниями. При этом физически (как объект) может существовать один центр, но технологически и информационно должна быть возможность организации работы виртуальных групп экспертов (участников ситанализа), необходимых для подготовки решений.

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.

СЦ и ИКР, как правило, включают в себя следующие модули:

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

КТС должен обеспечивать возможность приема (получения) и выдачи (отображения) разнородной информации, поступающей как из внутренних источников, так из внешних, представленной на различных носителях (компьютерная информация, видео и DVD носители, аудио информация, информация на бумажных носителях, карты, видеоконференция и т.п.).

ИАС должны обеспечивать 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 должна обеспечивать управление работой КТС и ИАС, а также предоставлять онлайн информационную и аналитическую поддержку в процессе обсуждения и принятия решений.

Возрастание информационного противоборства и рост информационных потоков во многом заставили переоценить как саму концепцию СЦ, так и способов их 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 СЦ была заложена технология data management (управления данными) или information management (управления информацией). По сути, деятельность СЦ сводилась к отображению информации для ее обсуждения по заранее спрогнозированному сценарию.

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

Практически от концепции «замкнутого» СЦ развитые страны переходят к концепции создания распределенных ситцентров, в которых сбор и агрегирование информации, а также генерация знаний осуществляется сообществом экспертов, получивших название collaboration system (системы взаимодействия) и intelligence sharing systems (системы обмена и распределения информации). В частности, создание таких систем ведется в силовых ведомствах США, госдепартаменте, корпорациях ВПК.

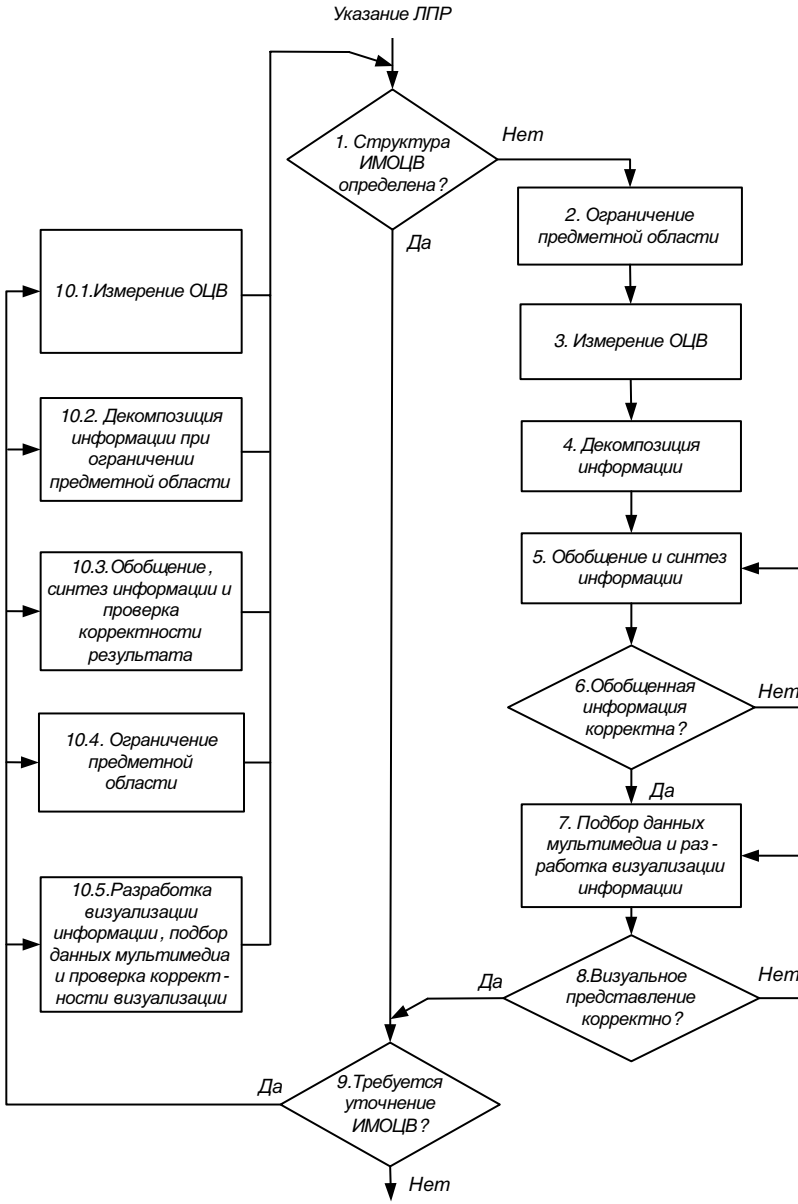
Технической основой таких систем является развитая защищенная телекоммуникационная среда и программные средства организации коллективной работы. Особое внимание уделяется системам управления знаниями, методикам и программам коллективного «мозгового штурма» (brainstorming) и генерации идей (idea generation), разрабатываются специальные методики презентации и представления информации.

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

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

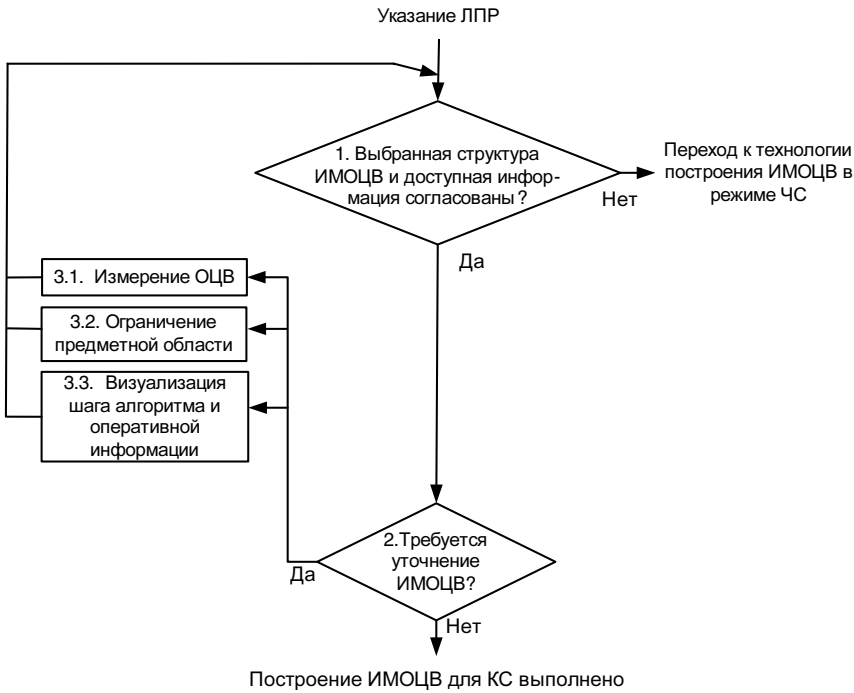
Резюмируя, можно сказать, что СЦ выступает в качестве инструмента, позволяющего лицу, принимающему решение (ЛПР), оперативно осмыслить проблему, разрешить ее неопределенность и способствовать достижению цели. Одной из важнейших особенностей современного КЦ является комбинация двух категорий технологий — информационных и управленческих, а также возможность работы в следующих трех режимах.

1. Исследовательский режим. Мониторинг объекта целевого воздействия (ОЦВ) и информирование 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 работы:

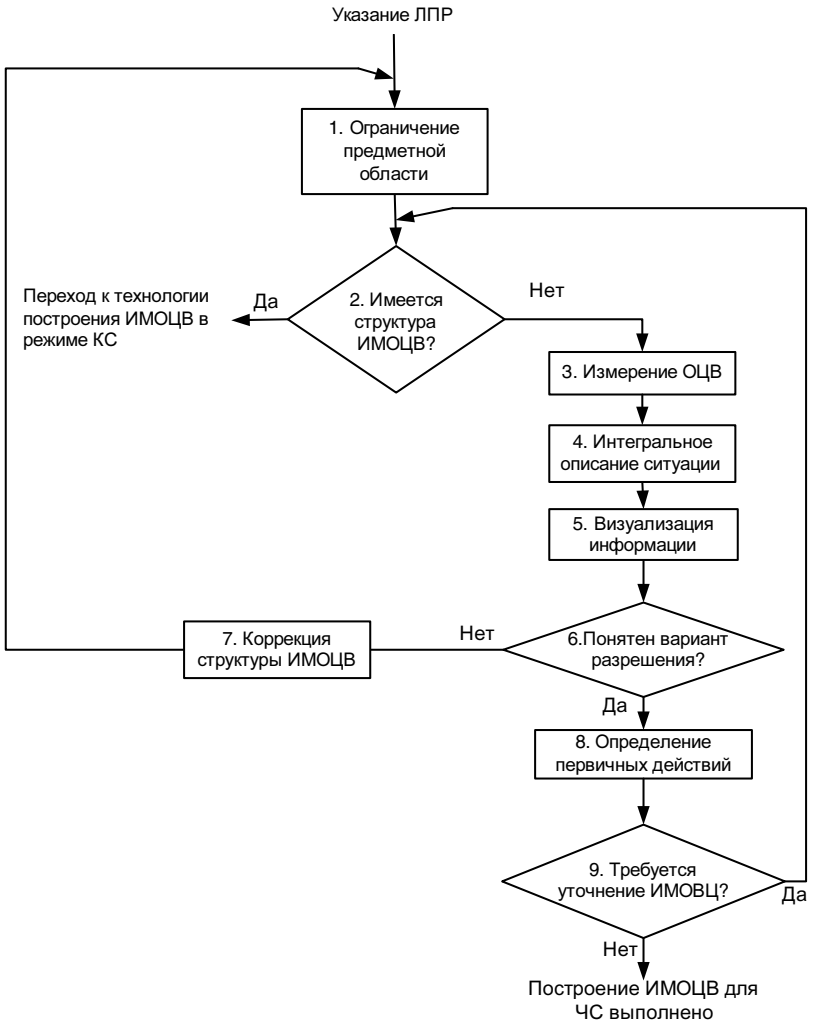


Построение ИМОЦВ в исследовательском режиме выполнено

2. *Кризисный режим* реализуемый в онлайне, когда на основе прецедентов и накопленной информации о фигурантах ситуации ИМОЦВ содержит готовые алгоритмы решений. Схема работы для кризисной ситуации (КС):



3. Чрезвычайный режим, протекающий в режиме онлайн, когда нет знаний о прецедентах, нет готовых алгоритмов решения и лимит времени весьма ограничен. Схема работы в чрезвычайной ситуации (ЧС):



Современные тенденции развития ситцентров за рубежом позволяют говорить о переходе госведомств и крупных корпораций к режиму электронного правительства и электронной компании и, соответственно, электронного СЦ.

4.3.3.3. Ситуационный центр Российской академии государственной службы при Президенте России

В качестве конкретного примера действующего ситцентра представляется оправданным воспользоваться СЦ Российской академии государственной службы при Президенте России (РАГС), информация о котором выложена в Интернете[14].

СЦ РАГС является автоматизированной информсистемой, предназначенной для обеспечения современными технологиями, программными и техническими средствами обработки и отображения информации коллективных действий группы лиц по решению проблем в масштабе времени, присущем коллегиям в органах госвласти и управления.

Ситцентр РАГС предназначен для выполнения следующих функций:

1. Поддержка ресурсами и средствами СЦ РАГС разнообразных активных форм проведения занятий со слушателями РАГС всех видов и форм обучения.

2. Поддержка ресурсами и средствами СЦ РАГС научно-исследовательских и информационно-аналитических работ, проводимых в РАГС.

3. Обучение персонала ситцентров использованию современных информационных, аналитических и технологических средств.

4. Проведение деловых игр по заявкам органов госвласти и местного самоуправления, коммерческих структур по проблемам, требующим применения интеллектуальных информационных технологий, в первую очередь, много- и междисциплинарным проблемам.

5. Стендовая отработка интеллектуальных информтехнологий и создание прототипов рабочих технологий федеральных органов власти.

В 2005 г. намечено:

- подключение СЦ РАГС к системе видеоконференций Центра дистанционного обучения;

[14] http://www.rags.ru/sitzent3.shtm

- установка специализированного сервера для локального и телекоммуникационного доступа к базам данных и другим ресурсам СЦ РАГС;
- выполнение НИР и оказание консультаций по тематике построения ситуационных центров и использования информационно-аналитических технологий.

На научно-практической конференции «Информационно-аналитические средства поддержки принятия решений и ситуационные центры» на базе РАГС (29-30 марта 2005 г.), состоялся заинтересованный обмен мнениями по различным аспектам внедрения ситцентров в органах госвласти, в т.ч. и об информационно-аналитических программах, о чем речь пойдет в следующем разделе[15].

4.3.3.4. Некоторые информационно-аналитические программы

Как в ситцентрах, так и вне их в систему управления все стремительнее внедряются информационно-аналитические системы (ИАС) и программы[16].

Так, отечественная ИАС **НЕВОД** предназначена для накопления, хранения и всестороннего анализа различной структурированной информации. НЕВОД — это инструмент построения информационно-аналитических систем, являющихся совокупностью удобных и мощных средств сбора и анализа разноплановой информации (текст, звук, видео, графика) из различных источников. Фактически НЕВОД представляет собой полнофункциональное информационное хранилище (Data Warehouse).

ИАС НЕВОД не требует от конечного пользователя никаких навыков программирования, она может быть настроена практически на любую предметную область, интересующую пользователя. Необходимая предметная область формируется один раз перед началом работы системы. Кроме того, при необходимости предметную область можно изменять в процессе работы с системой.

В НЕВОД легко настраивается пользовательский интерфейс, предусмотрен максимально легкий и быстрый способ построения отчетов и других форм для ввода и вывода информации. Кроме того, эти формы в процессе работы можно изменять. НЕВОД построен на ос-

---

[15] http://www.rags.ru/content.php?id=47

[16] См. Информационно-аналитические системы и средства поддержки организационного управления: Материалы научно-практической конференции / Под общ. ред. А.Н. Данчула. – М.: Издательство РАГС, 2004. – 188 с.

нове СУБД ЛИНТЕР и, по сути дела, является объектно-ориентированной надстройкой для реляционной СУБД ЛИНТЕР[17].

ИАС **«Семантический Архив»** компании «Аналитические бизнес-решения» реализует ряд очень важных функций для проведения аналитических исследований:

- ведение досье на объекты;
- организация единого хранилища фактографических данных;
- автоматизация выделения смысловых фрагментов (знаний) из текстов документов;
- организация хранилища знаний и электронной библиотеки документов;
- конструирование семантических отчетов.

ИАС функционирует следующим образом: наряду с документами и таблицами с данными, в информхранилище содержатся «карточки» на объекты, упомянутые в этих документах, «карточки» на отношения и действия этих объектов.

Поиск информации осуществляется по полям данных карточек: «кто купил акции», «когда произошел разрыв отношений» и т.д. Достигается это путем обработки данных документов с автоматическим извлечением из текста фактов упоминания объектов и автоматизированному извлечению (с участием операторов) упоминаемых в тексте отношений и действий. Поскольку свойства этих карточек индексируются системой, то поиск осуществляется мгновенно.

Основные функции ИАС:

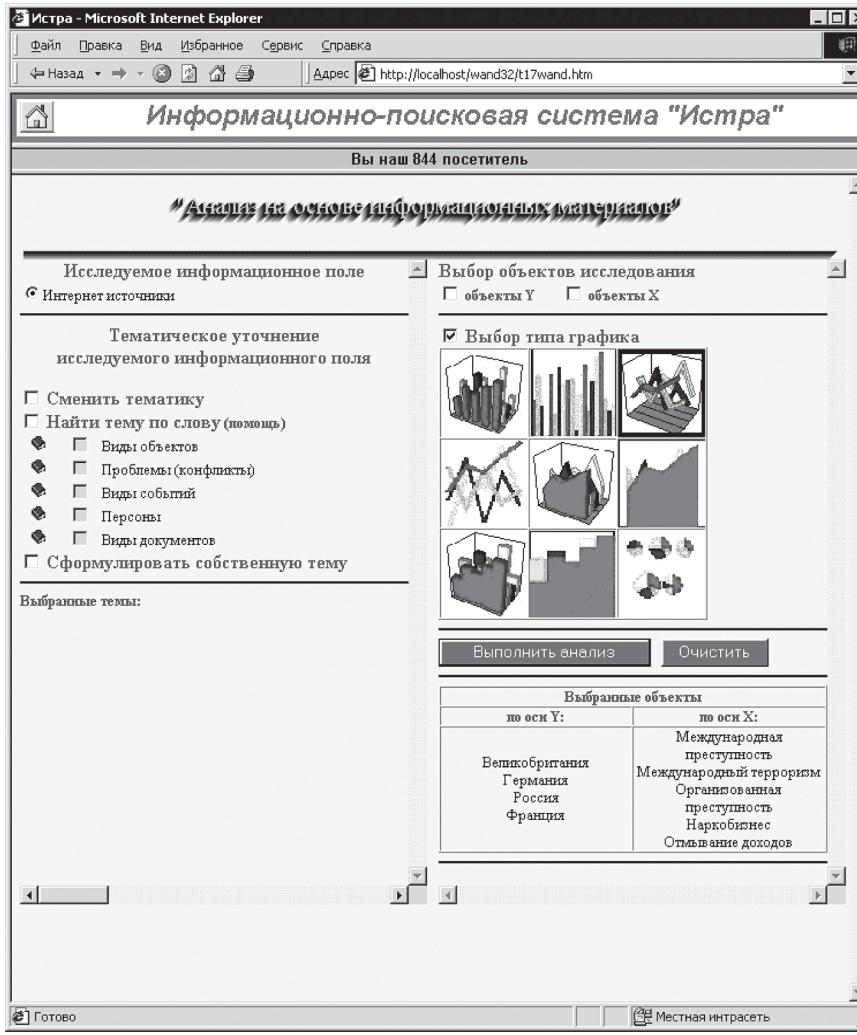
- мониторинг новостных сайтов с помощью специализированных роботов;
- периодическое импортирование информации из различных реляционных баз данных;
- индексация текстовой и фактографической информации, хранящейся в системе;
- полнотекстовый и параметрический поиск;
- Визуализация информации в виде таблицы документов, объектов или событий;
- визуализация параметров событий средствами бизнес-графики;
- визуализация событий и их привязка к карте;
- генерация новостных и аналитических дайджестов, отчетов и т. д.[18]

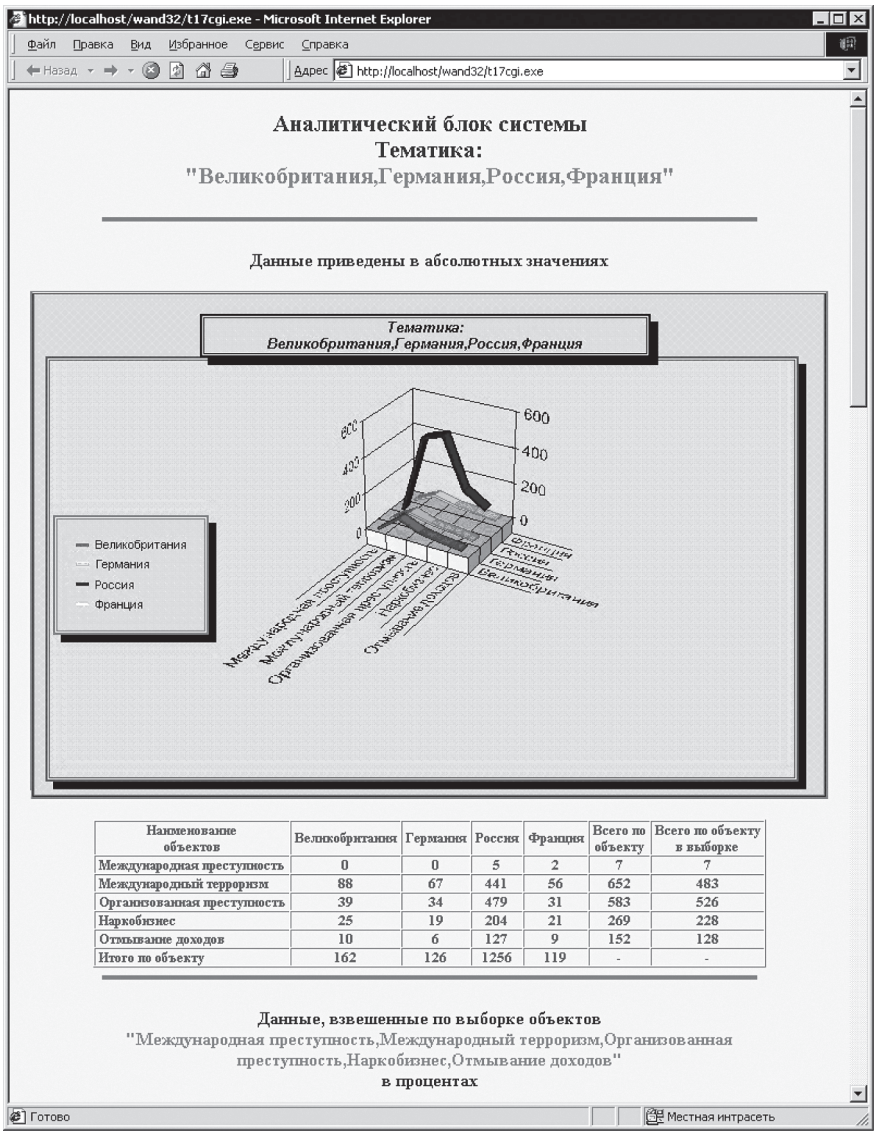
---

[17] http://www.relex.ru/rus/products/nevod/

[18] См. *Ульянова Т.* Инструментальные средства для представления семантики отображаемой информации// Материалы научно-практической конференции / Под общ. ред. А.Н. Данчула. – М.: Издательство РАГС, 2005.

Информационно-поисковая система «Истра» позволяет резко повысить полноту и оперативность информационного обслуживания пользователей. Это обеспечивается путем автоматического формирования в режиме постоянного мониторинга банка данных на основе информации из сети Интернет и других источников, а также поиска информации в сформированных банках данных с помощью моделей информационно-поисковых запросов и распределения информации по пользователям с учетом их информационных потребностей. Кроме того, ИПС «Истра» обеспечивает возможность ввода справочной информации и других необходимых документов (тексты международных договоров, аналитические справки, тексты законов, указов президента и постановлений правительства, приказов по ведомству и т.д.).


Истра - Microsoft Internet Explorer
Файл Правка Вид Избранное Сервис Справка
Назад
Адрес http://localhost/wand32/t17wand.htm
Информационно-поисковая система "Истра"
Вы наш 844 посетитель
"Анализ на основе информационных материалов"
Исследуемое информационное поле
Интернет источники
Тематическое уточнение исследуемого информационного поля
Сменить тематику
Найти тему по слову (помощь)
Виды объектов
Проблемы (конфликты)
Виды событий
Персоны
Виды документов
Сформулировать собственную тему
Выбранные темы:
Выбор объектов исследования
объекты Y
объекты X
Выбор типа графика
Выполнить анализ
Очистить
Выбранные объекты
по оси Y:
по оси X:
Великобритания
Германия
Россия
Франция
Международная преступность
Международный терроризм
Организованная преступность
Наркобизнес
Отмывание доходов
Готово
Местная интрасеть



Наименование объектов	Великобритания	Германия	Россия	Франция	Всего по объекту	Всего по объекту в выборке
Международная преступность	0	0	5	2	7	7
Международный терроризм	88	67	441	56	652	483
Организованная преступность	39	34	479	31	583	526
Наркобизнес	25	19	204	21	269	228
Отмывание доходов	10	6	127	9	152	128
Итого по объекту	162	126	1256	119	-	-

Базы данных по кризисам и конфликтам — системы CASCON, CRISIS обеспечивают возможность хранения в единообразной форме информации о различных конфликтах и кризисных ситуациях, проходивших в разных регионах, и ее оперативного извлечения.

Программное изделие «Баланс интересов» используется в процессе анализа международных конфликтов для прогнозирования их развития. Оно реализует прогнозную методику, основанную на использовании *модели процесса трансформации баланса интересов* объектов мировой политической системы. В основу моделирования положен подход, предполагающий оценку интересов объектов мировой политической системы путем их ранжирования по степени важности с использованием математического аппарата парных сравнений. При прогнозировании целью моделирования является получение срезов возможного состояния отношений исследуемых объектов мировой политической системы для выбранного сценария развития обстановки на основе учета трансформации баланса интересов. Подход обеспечивает возможность учета взаимодействия значительно большего числа факторов, объектов и характеристик, представления динамики поведения объектов, учета неопределенности и нечеткости информации, что, в свою очередь, повышает достоверность результатов проводимых исследований.

Интеллектуальная программа RCO Fact Extractor предназначена для эффективного решения задачи конкурентной разведки. Программа анализирует тексты на русском языке и находит в нем описания фактов (или артефактов) нужного типа, например, упоминания о встречах, договоренностях, приобретении собственности, классифицирует и упорядочивает их[19].

Основная сфера приложения программы – аналитические задачи из области компьютерной разведки, требующие высокоточного поиска информации, например, автоматический подбор материала к досье на целевой объект или же мониторинг определенных сторон его активности, освещаемых в СМИ. Помимо собственно программы с графическим интерфейсом для Windows выпускается пакет для разработки программного обеспечения (SDK), на базе которого построен Fact Extractor и который позволяет включать возможности анализа текста в собственные приложения.

Программа может обрабатывать документы в популярных текстовых форматах из различных источников – файловой системы, баз данных, заданных web-сайтов.

[19] http://www.rco.ru/article.asp?ob_no=1562

Скорость анализа документов зависит от количества объектов, по которым ведется мониторинг, и от частоты их упоминания в документах и находится в пределах от 15 до 100 Мб в час (при работе на Pentium-IV). Это позволяет производить оперативный анализ информации в реальном времени или ретроспективный анализ большого текстового массива, предварительно отфильтрованного при помощи любой поисковой машины.

Результат работы – таблица, которая содержит информацию о фактах, связанных с объектами мониторинга, и может экспортироваться в html-формат для формирования отчета или для загрузки в стороннее приложение, работающее с уже структурированными данными – первичными знаниями.

Третья версия инструмента компьютерной разведки RCO Semantic Network разработана компанией «Гарант-Парк-Интернет». Библиотека, выполненная в виде отдельной dll, может использоваться в разнообразных приложениях для анализа текста[20].

С помощью RCO Semantic Network 3.0 можно «выделять элементы смысла текста и их взаимосвязи, строить различного вида дайджесты». Особенно полезна она для информационных и PR-агентств, т.к. позволяет отслеживать информацию об определенных организациях и персонах, причем программа не только распознает различные варианты написания названий и фамилий, но может различать информацию об однофамильцах или организациях со схожими наименованиями

4.4. Перспективы информационного развития России

Правительство России 7 апреля 2005 г. рассмотрело и в целом одобрило проект программы развития инфраструктуры связи в России и поручило Мининформсвязи разработать совместно с Минэкономразвития, Минобрнауки, Минфином, Минобороны, МЧС, Минкультуры и Роскосмосом проект «Стратегии развития и использования информационных и коммуникационных технологий в Российской Федерации до 2010 года»[21].

Стратегия должна базироваться на «Концепции использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года» (рассмотрена выше).

Другими базовыми документами должны стать проект **«Национальной стратегии информационного развития»** и план **«Программы действий**

[20] http://www.lenty.ru/gocomp.html?http://www.oborot.ru/news/2826/11

[21] http://www.government.ru/data/structdoc.html?he_id=102&do_id=1864

по развитию информационного общества в России», подготовленные Центром развития информационного общества (РИО-Центр) в августе 2004 г. В этих документах сформулированы предложения по реализации комплекса мер нормативно-правового, политического, административного, экономического, социального и технологического характера, которые будут способствовать построению в России инфообщества, обеспечат экономический и социальный прорыв страны, поднимут уровень благосостояния, укрепят демократические институты и международный престиж России[22].

4.4.1. Национальная стратегия информационного развития

В стратегии отмечается, что Россия объективно втянута в процесс становления ГИО, ибо только доступ к материальным и духовным благам информационной цивилизации может обеспечить населению достойную жизнь, экономическое процветание и необходимые условия для свободного развития личности. Более того, чем прочнее наши связи с технологически развитыми странами, тем большее влияние мы сможем оказывать на мир, тем богаче источники нашего собственного экономического и технологического развития, тем успешнее обеспечена безопасность страны.

Известно, что становление инфообщества осуществляется через информационное развитие. Понятие *«информационное развитие»* в стратегии рассматривается как аналог таких понятий, как экономическое, социальное, политическое, технологическое и др. Оно означает трансформацию всех общественных институтов и сфер человеческой деятельности под воздействием ИКТ, прогресс во всех сферах разработки, производства и внедрения ИКТ, создание политических, экономических, правовых, социальных и научно-технических условий для формирования развитой информационной среды, адекватной задачам социально-экономического развития страны, подготовку граждан, общественных институтов, бизнеса и органов госвласти всех уровней к жизни в условиях информационного общества.

Базовые, конечные **цели информационного развития России,** по мнению авторов стратегии, состоят в следующем:

- *укрепление федеративного государства* на основе единого информационного пространства страны, углубление процессов информационной и экономической интеграции регионов;

[22] http://sr.fondedin.ru/new/fullnews.php?subaction=showfull&id=1095935196&archive=1095935540&start_from=&ucat=14&

- *создание современных сетевых структур государственного, регионального и муниципального управления* и построение на их базе новых эффективных механизмов взаимодействия власти с институтами гражданского общества, бизнесом и населением;
- *становление и в последующем доминирование в экономике новых технологических укладов*, базирующихся на массовом использовании перспективных ИКТ, средств вычислительной техники и телекоммуникаций, ведущей роли информационно-коммуникационной инфраструктуры в системе общественного производства, в социальной и культурной сферах;
- *повышение качества образования, уровня научно-технического и культурного развития* за счет расширения возможностей информобмена на международном, национальном и региональном уровнях;
- *повышение роли квалификации, профессионализма и способностей к творчеству* как важнейших характеристик услуг труда, а также *достижение высокого уровня минимальной социальной обеспеченности;*
- *создание системы обеспечения прав граждан и общественных институтов на свободное получение, распространение и использование информации* как важнейшего условия демократического развития;
- *обеспечение высокого уровня национальной безопасности* за счет предотвращения террористических и криминальных угроз в инфосфере.

Как уже отмечалось (см. глава 1) информационная глобализация порождает и целый комплекс *негативных геополитических последствий*. Прежде всего, это ускорение поляризации мира, увеличение разрыва между богатыми и бедными, технологически передовыми и отсталыми странами, что является главным источником нестабильности и конфликтов.

Разные страны и социальные группы, по причинам экономического и политического характера, имеют неравные возможности доступа к мировым информресурсам, приобретению и использованию современных ИКТ, что порождает цифровое неравенство. Для России с ее огромной территорией и низким уровнем развития инфраструктуры ИКТ в отдаленных регионах характерно *информационное неравенство центра и регионов*. Его преодоление является важнейшим условием укрепления политического и экономического единства страны, ускоренного экономического и социального развития и обеспечения безопасности.

Опережающее информационное развитие имеет для страны важное геополитическое значение. Россия, занимая исключительное географическое положение, является естественным мостом между

Европой и Азиатско-Тихоокеанским регионом (АТР). Создание инфраструктуры ИКТ на всей территории нашей страны, и в первую очередь в Сибири и на Дальнем Востоке, позволит повернуть основные потоки экономического и культурного обмена между АТР и Европой через территорию России, привлечь российские и зарубежные капиталы для развития этих регионов.

4.4.1.1. Предпосылки и проблемы информационного развития

В стратегии отмечается, что за последние годы в стране созданы серьезные предпосылки для формирования основ инфообщества:

- сформировался и быстро развивается отечественный рынок ИКТ, продуктов и услуг;
- сформировано сообщество компаний и фирм, ведущих профессиональную деятельность на рынке ИКТ и обслуживающих все сегменты этого рынка;
- российскими компаниями накоплен определенный опыт реального производства товаров и услуг, использующих современные ИКТ;
- создан базис для законодательного и нормативного обеспечения развития ИКТ;
- в значительной степени компьютеризированы многие отрасли хозяйства, в частности банковская сфера и сфера госуправления;
- в общественном мнении складывается понимание актуальности задачи использования ИКТ в реальном бизнесе, в политике и управлении, в здравоохранении и культуре, в науке и образовании и т. д.

Тем не менее, в информразвитии имеются заметные недостатки:

- малая эффективность координации и экспертизы госпрограмм и проектов информатизации, создаваемых за счет госбюджета;
- практическое отсутствие системы мониторинга процессов информатизации и невозможность проведения полноценного статистического наблюдения за развитием и использованием ИКТ;
- слабость и фрагментарность действующего информационного законодательства и нормативного правового обеспечения процессов информатизации, существенно затрудняющего работы по созданию электронного правительства и ведению электронного бизнес.

Высокий уровень образования населения создает благоприятные предпосылки для информразвития. Россия находится на уровне экономически развитых стран. Растет число студентов, получающих образование в сфере ИКТ, и по их числу, приходящемуся на 1000 чело-

век, Россия не уступает таким странам, как Франция, Швеция и Германия.

Что касается кадровой составляющей, то, как отметил журнал «CIO», очень важной является задача создания в стране института главного правительственного специалиста по информационным технологиям, верховного государственного ИТ-начальника или, иначе говоря, CIO национального масштаба[23].

4.4.1.2. Приоритетные направления и механизмы информационного развития

Сформулированные выше стратегические цели и трезвая оценка сложившихся предпосылок движения страны к инфообществу позволяют выделить следующие приоритетные направления информразвития.

1. Опережающее развитие инфраструктуры ИКТ.

Развитие и модернизация информационно-коммуникационной инфраструктуры (ИКИ) составляет технологическую базу экономического, социально-политического и культурного развития страны и является приоритетом информразвития. ИКИ представляет собой совокупность территориально распределенных государственных и корпоративных ИВС, телекоммуникационных сетей (каналов передачи данных, средств коммутации и управления информпотоками), информресурсов, хранящихся, обрабатываемых и передаваемых в электронной форме, а также оргструктур, правовых и нормативных механизмов.

Реализация данного приоритетного направления связана с необходимостью модернизации и дальнейшего развития:

- существующей технологической базы Взаимоувязанной сети связи России (ВСС) и входящих в ее состав национальных и корпоративных инфокоммуникационных сетей и систем;
- системы национальных информресурсов и технологий доступа к ним;
- российского сегмента Интернета;
- центров обработки информации различного назначения.

2. Развитие отечественного рынка ИКТ, информпродуктов и услуг.

Сегодня превалирует ориентация на использование, в т.ч. и в органах госвласти, зарубежной техники и ИКТ. На современном этапе

[23] http://www.cio-world.ru/offline/2004/31/36990/

это единственный путь внедрения ИКТ однако этот путь может привести нашу страну к зависимости от иностранных производителей, что негативно скажется на развитии страны и ее безопасности. Поэтому одной из важнейших задач является становление отечественной отрасли ИКТ, максимальное удовлетворение потребности общества в высококачественной технике, программных продуктах и услугах, уменьшение зависимости от зарубежных производителей, завоевание ниши на мировом рынке ИКТ.

Реализация этого перспективного направления предполагает активное участие государства, которое должно создать привлекательные для бизнеса и всего общества экономические, правовые, социальные, организационные и другие условия для стимулирования отечественных производителей и продвижения российской продукции на внутренний и мировой рынки.

3. Широкомасштабное использование ИКТ в сфере госуправления.

Реализация этого направления призвана существенно улучшить деятельность аппарата управления за счет перехода на электронный документооборот, интеграции в единую вертикальную сеть корпоративных сетей министерств и ведомств, а также системы распределенных регулярно обновляемых баз данных управленческой информации внутри каждого ведомства, в короткие сроки завершить функциональную и структурную перестройку аппарата управления, начатую в административной реформе.

Будут созданы реальные условия для предоставления гражданам и организациям общедоступной правительственной, административной и правовой информации, повысить результативность интерактивного взаимодействия между собой органов власти на всех уровнях системы госуправления, а также их диалога с гражданами, с субъектами экономической деятельности, с институтами гражданского общества, сделать госуправление более ответственным и открытым.

В результате будет достигнуто существенное продвижение страны по пути демократизации, реализована платформа ЭП как ответ государства на вызов информационной эпохи в политической сфере.

4. Обеспечение информационной безопасности страны.

Глобальная информатизации и развитие Интернета привели к тому, что ИКИ страны и национальные информресурсы оказались весьма уязвимыми объектами для воздействия недружественных государств, террористических организаций, криминальных групп и отдельных злоумышленников. Угроза международного информационного терроризма и информационных войн стали важными геополитическими факторами.

В процессе реализации этого направления в стране должна быть создана единая многоуровневая система обеспечения информбезопасности, в которой действуют единые правовые нормы и механизмы защиты информресурсов, ИКИ и информационных прав граждан, осуществляется эффективная координация деятельности федеральных органов госвласти и других организаций (подробнее – в главе 5).

5. Международное сотрудничество в сфере ИКТ.

Важнейшей целью международного сотрудничества в сфере ИКТ является создание информационного миропорядка, отвечающего национальным интересам России. В ГИО, где будет обеспечено широкое представительство по-разному политически ориентированных как развитых, так и развивающихся стран, интересы России — поставщика и потребителя ИКТ — должны быть учтены наиболее полно. Поэтому России необходимо активно включаться в разработку и практическое формирование концепции ГИО, ее принципов и структуры.

Россия выступает за равное партнерство развитых и развивающихся государств в вопросах создания инфообщества, за свободный, не дискриминационный доступ к современным ИКТ. Необходимо создать условия добросовестной конкуренции и стимулирования инвестиций на рынке информационно-коммуникационных услуг.

Международное сотрудничество должно обеспечить условия, при которых глобальная информатизация не наносила бы ущерб национальной безопасности, суверенитету, культуре и самобытности всех стран, в том числе и России, и была бы обращена на решение социально-экономических и гуманитарных проблем человечества, отдельных регионов и стран.

Важным направлением международной деятельности в области ИКТ остается выстраивание двусторонних связей на основе межправительственных и межведомственных соглашений и работа со всем спектром международных организаций, имеющих отношение к техническим, экономическим, политическим, правовым и прочим аспектам применения ИКТ, а также участие в телекоммуникационных форумах.

6. Совершенствование и развитие нормативно-правового регулирования процессов информационного развития.

Нормативно-правовое регулирование есть главный рычаг воздействия на все направления информационного развития. Поэтому государство должно играть активную роль в нормативно-правовом регулировании отношений, связанных с формированием развитой информационной среды.

Должны быть закреплены правовые гарантии реализации конституционных прав граждан на получение информации и обеспечение доступа граждан к информации о деятельности органов госвласти и МСУ, а также решениях, затрагивающих их права, свободы и законные интересы. Должна быть обеспечена защита конфиденциальной информации, права на неприкосновенность частной жизни, личную и семейную тайну. Должно быть обеспечено правовое регулирование в области формирования, хранения и использования национальных информресурсов и усовершенствованы нормы, регулирующие ответственность за правонарушения в сфере производства, хранения, распространения и использования информации.

Дальнейшему совершенствованию подлежат институты защиты интеллектуальной собственности в области производства и потребления информации, прежде всего, прав производителей, распространителей и пользователей ИКТ, информационных продуктов и услуг.

Должны быть решены вопросы правового регулирования использования сети Интернет.

Исходя из оценки состояния социально-экономического развития России, наиболее актуальными для информационного развития на период до 2008 г. определены первые три из перечисленных направлений. Для их реализации в стратегии поставлены следующие задачи:

1. Покрытие всей территории страны телекоммуникационными сетями, использующими современные и перспективные ИКТ, как главное условие преодоления информационного неравенства центра и регионов.

2. Технологическое переоснащение существующих сетей и систем телекоммуникаций и связи с их ориентацией на предоставление универсальной услуги.

3.Разработка единых стандартов взаимодействия информсистем, в том числе государственного назначения.

4. Усиление межведомственной координации при создании информсистем государственного назначения.

5. Разработка общегосударственной системы формирования, хранения, предоставления и защиты национальных информресурсов и совершенствование технологий доступа к ним.

6. Развитие системы пунктов общественного доступа к открытым информационным сетям, Интернету, информресурсам и ИКУ.

7. Обеспечение безопасности критически важных сегментов и объектов ИКИ и разработка системы управления информбезопасности для ИКИ.

В части развития отечественного рынка ИКТ, информационных продуктов и услуг в стратегии определены следующие задачи:

1. Анализ научно-производственного и технологического потенциалов российских предприятий и выявление направлений и видов конкурентоспособной продукции для внутреннего и внешнего рынков.

2. Разработка системы мер экономического и административного регулирования и правовых механизмов, стимулирующих отечественного производителя в выбранных направлениях и видах.

3. Создание условий для активного продвижения отечественных ИКТ, информационных продуктов и услуг на внутреннем и мировом рынках.

4. Развитие системы предоставления комплекса социальных услуг всем гражданам страны.

5. Стимулирование развития рынка инфокоммуникационных услуг.

6. Господдержка и стимулирование всех видов электронной коммерции.

7. Совершенствование нормативно-правовой базы функционирования рынка ИКТ, информационных продуктов и услуг.

В части масштабного использования ИКТ и сетевых телекоммуникаций в сфере госуправления должны быть решены следующие задачи:

1. Формирование госполитики в области использования ИКТ в органах власти всех уровней.

2. Разработка нормативно-правовой базы создания и функционирования ЭП.

3. Интеграция госинформресурсов и развитие систем доступа к ним.

4. Создание систем ЭДО в органах госвласти всех уровней и регламентов их информационного взаимодействия.

5. Обеспечение эффективного взаимодействия органов госвласти с населением.

6. Обеспечение информбезопасности ИКТ сетей систем органов госвласти.

4.4.2. Практические задачи развития ИКТ на ближайшую перспективу

В апреле 2005 г. состоялось Всероссийское совещание отрасли информационных технологий и связи, на котором были подведены итоги 2004 г. и уточнены задачи ее развития на ближайшую перспективу. В докладе министра Л.Д.Реймана было подчеркнуто, что ИКТ

приобрели критическую важность для повышения эффективности госуправления, обеспечения национальной безопасности, адресной социальной помощи, совершенствования систем образования и здравоохранения[24].

В 2004 г. отрасль ИКТ сохранила высокие темпы роста. Рост объема рынка в 2004 г. составил 30,5%, что более, чем в четыре раза выше общих темпов роста экономики.

Такое развитие привело к росту доли ИКТ в ВВП по отношению к 2000 г. — с 3,2% до 4,9%. Однако, несмотря на достигнутые темпы развития рынка, в целом по уровню проникновения ИКТ Россия отстает от многих развитых стран. Роль информации как экономического ресурса неуклонно растет, и именно отрасль ИКТ становится локомотивом развития постиндустриальной экономики. Объем российского рынка ИКТ в 2004 г. оценивается в 255,6 млрд руб., что на 20 процентов выше показателей 2003 г.

[24] http://www.minsvyaz.ru/site.shtml?id=3202

Высокие темпы роста демонстрирует рынок услуг связи. За последние пять лет этот рост ежегодно составлял около 40 процентов. За 2004 г. объем рынка составил 540,0 млрд руб., что на 37% выше показателей 2003 г.

В результате проведенной в 2004 г. административной реформы были разделены функции по формированию и реализации государственной политики в сфере развития и использования ИКТ.

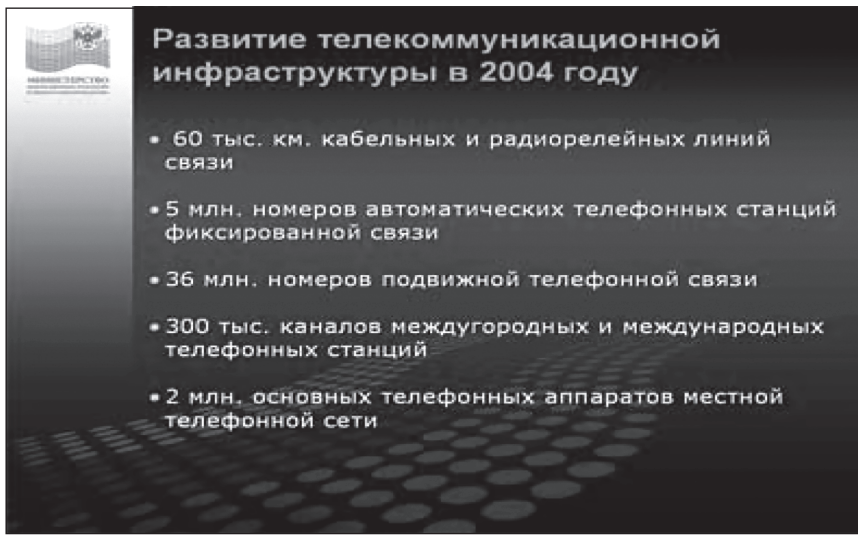
При этом задачи, возложенные на блок, подведомственный Мининформсвязи, существенно расширились, что отражает возросшую роль ИКТ в государственном управлении и социально-экономической сфере.

По оценке министра, ключевым событием для отрасли в 2004 г. стало вступление в силу Федерального закона «О связи». В его основу положен принцип создания равных условий для доступа граждан России к услугам связи. Постановления правительства, устанавливающие порядок применения закона «О связи» формировались в течение всего 2004 г. В результате созданы условия для дальнейшей либерализации рынка телекоммуникаций.

С 2005 г. начинается внедрение механизма универсального обслуживания, используемого в большинстве стран. Этот подход позволит решить до сих пор актуальную проблему телефонизации удаленных населенных пунктов, где недостаточная плотность населения делает развитие инфраструктуры связи экономически невыгодным.

В целях активного продвижения России к инфообществу, наряду с уже рассмотренными, разработаны несколько ключевых документов. Так, в «Концепции развития рынка информационных технологий» определены основные направления обеспечения господдержки развития национального производства ИКТ, конкурентоспособных на мировом рынке, и превращение их в одну из основных движущих сил экономического роста страны.

В «Концепции региональной информатизации до 2010 года» сформулированы основные задачи и направления внедрения ИКТ в целях социально-экономического развития субъектов Федерации, совершенствования регионального и муниципального управления.



Рост рынка телекоммуникаций сопровождался развитием и модернизацией инфраструктуры. Телефонизация увеличилась за год с 26,6 до 28,8 стационарных телефонных аппаратов на 100 человек. Количество нетелефонизированных населенных пунктов сократилось с 50 до 46 тысяч.

В соответствии с ФЦП «Социальное развитие села до 2010 года» в 2004 г. продолжено развитие сельской телефонной связи, где введено в эксплуатацию 600 тыс. номеров, что на 69% больше, чем в 2003 г.

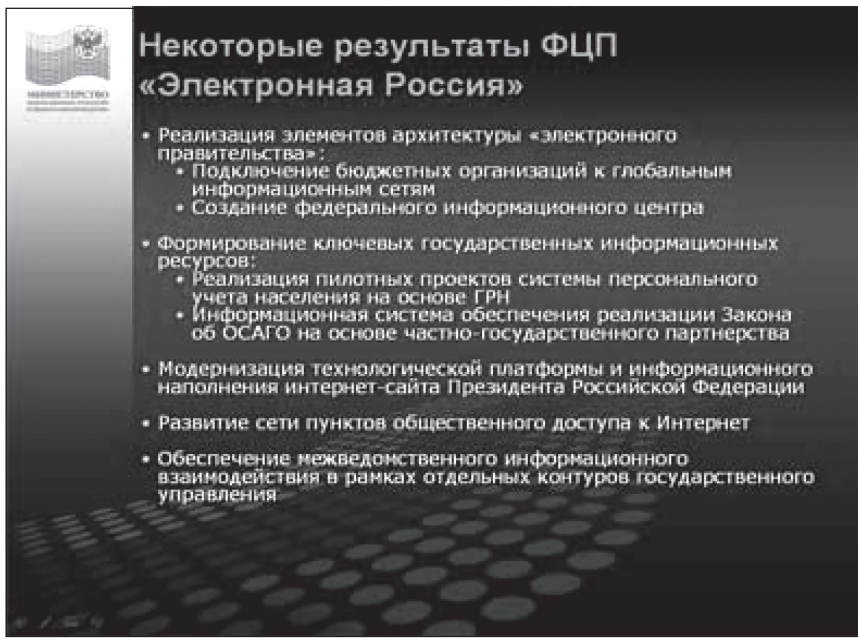
Впечатляют темпы роста мобильной связи: на конец 2004 г. количество абонентов составило 72,0 млн — в 2 раза больше по сравнению с 2003 г. Уровень охвата подвижной связью составил 50 телефонных аппаратов на 100 человек, а в Москве в начале 2005 г. превысил 100%. К концу 2005 г. количество сотовых телефонов превысит сто миллионов.

Работы по созданию космических аппаратов нового поколения серии «Экспресс-АМ». Введенные в эксплуатацию 5 спутников этой серии завершили в 2005 г. обновление российской спутниковой группировки и позволили ФГУП «Космическая связь» войти в десятку ведущих международных операторов спутниковой связи. Следующий этап модернизации намечен на 2007 г.

В 2004 г. продолжилось проникновение ИКТ в социально-экономическую сферу. Количество пользователей сети Интернет возросло на 32% и составило более 18 млн человек. Каждый восьмой житель России пользуется услугами всемирной сети, при этом в Москве — каждый второй.

Однако, несмотря на относительно высокие темпы роста, многие эксперты оценивают степень готовности России к инфообществу как недостаточную. Рынок ИКТ, структура формируется во многом за счет продаж импортируемого аппаратного и ПО. Отечественное конкурентоспособное производство в этой сфере только формируется.

В рамках Программы также предполагается поддержать российские компании при их выходе на мировой рынок, устранить административные барьеры и создать дополнительные стимулы для их развития. В рамках программы предусмотрено также создание новых механизмов привлечения инвестиций в развитие российских предприятий в сфере ИКТ через формирование специального венчурного фонда.



Относительно реализации ФЦП «Электронная Россия» министр отметил, что в 2004 г. Программа была профинансирована на 15,2% от объемов, предусмотренных ее паспортом, что заставило сосредоточиться на приоритетных проектах. Так, начата работа по созданию госсистемы изготовления, оформления и контроля паспортно-визовых документов с использованием биометрической информации. Продолжены работы по созданию госрегистра населения и его интеграции с ведомственными автоматизированными системами, содержащими персональные данные о населении страны. Ведется реализация ряда крупных инфраструктурных проектов, направленных на формирование телекоммуникационной инфраструктуры для госнужд. Создается федеральный информационный центр, формируется сеть удостоверяющих центров в области электронной цифровой подписи.

Продолжено развитие пунктов общественного доступа к открытым информресурсам, в т.ч. к сети Интернет. В 2004 г. количество посещений пунктов коллективного доступа ФГУП «Почта России» составило 3,5 миллиона.

Мининформсвязи (совместно с Минэкономразвития) **готовит новую редакцию ФЦП**. В 2005 г. будет продолжена реализация приоритетных проектов, прежде всего по созданию элементов ЭП, имеющих межведомственное значение.

Важным направлением останется совершенствование нормативно-правовой базы, которое будет развиваться в следующих трех направлениях:

- обновление и совершенствование базового законодательства;
- коррекция и доработка правовых норм, регулирующих отдельные направления деятельности отрасли;
- поправки в законодательство, соответствующие специфическим интересам экономического развития отрасли.

По каждому из них у Мининформсвязи сформирована программа действий. Так, федеральные законы «Об информации, информатизации и защите информации», «О средствах массовой информации», «О рекламе» приняты более 10 лет назад и требуют их актуализации.

Новыми для госрегулирования стали вопросы, связанные с использованием **глобальной сети Интернет**. В этой части необходимо:

- раскрыть правовые вопросы использования ИКТ для дистанционного предоставления социально значимых услуг (образовательных, медицинских, юридических);
- дать правовое определение электронных СМИ, распространяемых через Интернет;

- узаконить средства борьбы с навязываемым распространением информации («спамом»).

В этих целях гармонизировать базовые российские законы с мировой практикой, принять **Федеральный закон «Об электронной торговле»,** скорректировать Федеральный закон **«О конкурсах на размещение заказов на поставки товаров, выполнение работ, оказание услуг для государственных нужд»** так, чтобы уравнять процедуры электронных госзакупок с традиционными.

Самоочевидно, что без данных законов невозможно использовать потенциал Интернета для бизнеса, эффективной деятельности органов госвласти и повышения качества предоставляемых гражданам госуслуг.

При этом совершенствование правовой базы в сфере электросвязи также должно обеспечить следующее:

- предоставить пользователям сетей подвижной связи **гарантии сохранения за потребителем номера телефона при смене оператора связи;**
- обеспечить адекватный правовой режим для работы **виртуальных операторов подвижной связи —** компаний, не обладающих собственным частотным ресурсом, но предоставляющих от своего лица услуги связи;
- навести порядок в лицензировании услуг связи для целей кабельного и эфирного вещания, **разделить лицензирование доступа к эфиру и лицензирование собственно информационного содержания программ;**
- продолжить работа по либерализации рынка услуг связи, в частности по демонополизации междугородней и международной связи, что обеспечит свободу конкуренции и приведет к существенному снижению тарифов.

Мининформсвязи России 22 июня 2005 г. внесло в Правительство России уточненный проект государственной программы «Создание в Российской Федерации технопарков в сфере информационных технологий». Проект программы был разработан совместно с Минэкономразвития России, Минобрнауки России и Минфином России при активном участии отраслевых ИТ-ассоциаций в рамках поручения Президента Российской Федерации В.В. Путина по итогам совещания в Новосибирске 11 января 2005 г.

В проекте Программы (см. приложение) рассмотрены вопросы формирования инфраструктуры технопарков, развития механизмов управления, мониторинга, коммерциализации результатов их деятельности, прогнозирования и стратегии их развития, подготовки высо-

коквалифицированных кадров, а также отражены необходимые объемы финансирования.

Предполагается, что в рамках реализации государственной программы будет создано 5 специализированных технопарков на территории Новосибирской, Нижегородской, Московской областей и Санкт-Петербурга. Данные регионы являются пилотными для отработки организационных, финансовых и законодательных механизмов создания и функционирования в России технопарков в сфере ИТ.

В дальнейшем решение о создании технопарка, в том числе за счет средств федерального бюджета, должно приниматься на федеральном уровне на конкурсной основе по результатам анализа заявок регионов, содержащих данные о предлагаемых для строительства земельных участках, бюджетном софинансировании и привлеченных инвестициях.

Технопарки могут размещаться, в том числе на территориях, обладающих статусом особых экономических зон.

Финансирование указанной программы может осуществляться, начиная с 2006 г. по 2010 г., при принятии решения Правительством России. Проект программы предусматривает общий объем финансирования мероприятий в размере около 123 млрд рублей, в т. ч. из средств:

- федерального бюджета около 20 млрд рублей (16%);
- субъектов Российской Федерации около 15 млрд рублей (12%);
- внебюджетных источников около 88 млрд. рублей (72%).

В результате реализации программы общий объем производства ИТ отрасли в 2010 г. в России может составить около 1 трлн рублей в год.

Предполагается, что будет создано до 100 тыс. рабочих мест для квалифицированных специалистов, в т.ч. из стран СНГ, а Россия может войти в тройку лидеров на мировом рынке ИТ-аутсорсинга. На основании развитой инфраструктуры технопарков международные компании откроют в России исследовательские и производственные центры.

Президент Российского научного центра «Курчатовский институт» академик Е. Велихов подчеркнул, что в 2007 г. действующие и создаваемые российские технопарки составят серьезную конкуренцию аналогичным зарубежным центрам научной поддержки развития ИКТ[25].

[25] http://www.newseducation.ru/news/2/20050118/8892.shtm

Программа «**Развитие национальной инфокоммуникационной инфраструктуры Российской Федерации**» — направлена на решение 6 проблем.

- **Конверсия радиочастнотного спектра.** В России менее 10% частотного спектра выделено для гражданского применения (по сравнению с 70% в других странах). Проведение конверсии создаст условия для развития перспективных радиотехнологий и отечественной промышленности.
- **Развитие цифрового телевидения.** Внедрение технологии DVB повышает число передаваемых программ в несколько раз без дополнительного частотного ресурса и при многократно меньшей мощности передатчика.
- **Развитие цифровой выделенной сети связи для нужд госуправления, обороны, безопасности и правопорядка,** которая обеспечит госорганам устойчивую, надежную и безопасную инфраструктуру связи самого современного уровня.
- **Развитие единой сети навигационно-временного обеспечения.** Ее создание позволит повысить эффективность решения самых разных задач, например,— повышения качества синхронизации в сетях связи.
- **Создание единой службы экстренного оперативного вызова.** Такая служба позволит быстро и гарантированно (и, разумеется, бесплатно для вызывающего) связаться с диспетчерской службой через единый номер. Это — необходимая гарантия безопасности жизни и здоровья граждан.
- **Модернизация почтовой связи.** Без использования современных технологий почтовая инфраструктура не сможет работать лучше.

В 2005 г. приоритетными целями госполитики в сфере ИКТ определены следующие:

- создание условий для их широкого распространения и эффективного использования в социально-экономической сфере и госуправлении;
- обеспечение растущих потребностей населения и организаций в современных инфокоммуникационных сервисах на всей территории;
- превращение национального производства в сфере ИКТ в одну из основных движущих сил экономического роста страны.

Решение перечисленных задач позволит в 2005 г. достичь объема рынка услуг связи более 700 млрд руб., или с ростом к предыдущему году на 30%. Российский рынок ИТ может превысить 300 млрд рублей и тем самым войти в десятку крупнейших европейских ИТ-индустрий.

В конце июня 2005 г. Президент России В.Путин поручил Правительству РФ[25] рассмотреть вопрос о создании специализированной организации – инвестиционного фонда технологий и инноваций, а

[25] «Коммерсант». 2005. 7 июля.

по сути, государственного венчурного фонда. Подготовка проекта поручена Мининформсвязи, Минфину и Минэкономразвития РФ. Фонд будет представлять собой ОАО, 76% акций которого принадлежат государству, а 24% – зарубежным инвесторам. Характерно, что на этапе создания фонда оговаривается его дальнейшая приватизация. Планируется, что уже к 2008 г. государство продаст акции фонда (оставит себе около 24% акций).

С учетом потенциальных зарубежных инвестиций первоначальный размер фонда может составить $100 млн. За три года за счет продажи акций фонда частным инвесторам его капитал увеличится до $300-400 млн. Эксперты считают, что размер инвестиций, направленных в российский ИТ-бизнес через фонд, в ближайшие три года составит $1,2–1,6 млрд. Среди кандидатов — производитель систем распознавания текста ABBYY, новосибирский разработчик софта SW-Soft, разработчик биометрических средств распознавания avision, а также другие фирмы.

Глава 5
НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ РОССИИ В УСЛОВИЯХ ИНФОРМАЦИОННОЙ ГЛОБАЛИЗАЦИИ

ИКТ уже привели к революции в военном искусстве. Неизбежно, что революционным изменениям подвергнется и сфера дипломатии.

5.1. Информационная революция и новые угрозы

Под воздействием информационной революции цивилизация столкнулась с вызовами и угрозами безопасности принципиально нового характера. Рассмотрим основные из них.

5.1.1. Вирусы и шпионские программы

Классификация вирусов и шпионских программ — предмет специальных исследований. В последнее время данной проблеме уделяется повышенное внимание и в компьютерной периодике. Для большинства пользователей наиболее известна и понятна вирусная проблема, с которой они обычно сталкивались лично.

5.1.1.1. Компьютерные вирусы и их классификация

Вирус — это самовоспроизводящаяся программа. Такая способность является единственным средством, присущим всем типам вирусов. При этом любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса могут вообще не совпадать с оригиналом.

Вирус не может существовать в «полной изоляции»: трудно представить вирус, который не использует код других программ, информацию о файловой структуре или просто имена других программ. Причина понятна: вирус должен обеспечить передачу себе управления.

В настоящее время количество программных вирусов приближается к 100 тыс. Их можно классифицировать по следующим признакам:

- среде обитания;
- способу заражения среды обитания;
- воздействию;
- алгоритму.

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные.

- Сетевые вирусы распространяются по компьютерным сетям.
- Файловые вирусы внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению.
- Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record).
- Файлово-загрузочные вирусы заражают и файлы, и загрузочные секторы дисков.

По способу заражения вирусы делятся на резидентные и нерезидентные.

- Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти вплоть до выключения или перезагрузки компьютера.
- Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы делятся на следующие виды:

- неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках. Их действие проявляются в каких-либо графических или звуковых эффектах;
- опасные вирусы, которые могут привести к различным нарушениям в работе компьютера;
- очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям **алгоритма** вирусы трудно классифицировать из-за большого разнообразия. Простейшие вирусы — **паразиты** — изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и удалены. **Вирусы-репликаторы, называемые червями**, распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии. **Вирусы-невидимки**, или стелс-вирусы, очень трудно обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. Наиболее трудно обнаружить **вирусы-мутанты**, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

Так называемые квазивирусные или **«троянские»** программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков. В качестве свежего примера рассмотрим программу Sikou.A, использующую для распространения Microsoft Word.

Троянец эксплуатирует уязвимость MS03–037 в приложениях Microsoft Office, позволяющую выполнять произвольный код на системе. Sikou.A устанавливает себя на компьютер при открытии зараженного файла Word. Он копируется в системный каталог и устанавливает 2 файла, один из которых несет троянский функционал, а другой служит для сокрытия вредоносной активности, что делает ее обнаружение чрезвычайно трудной.

Вирус связывается с URL, на котором получает инструкцию, с каким URL связываться дальше. Соединившись со вторым URL, вредоносный код скачивает файл, расширяющий его функции, и затем

соединяется с третьим URL, откуда получает команды на сбор информации и загрузку программ[1].

«Полиморфный вирус» представляется на сегодня наиболее опасным, т.к. он модифицируют свой код в зараженных программах так, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите. Такие вирусы не только шифруют свой код, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика. Полиморфные вирусы — это вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования: имея зараженный и оригинальный файлы, вы все равно не сможете проанализировать его код с помощью обычного дизассемблирования. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны варианты: он может расшифровать себя всего сразу, а может выполнить такую расшифровку «по ходу дела», может вновь шифровать уже отработавшие участки.

Если вирусы и «троянские кони» наносят ущерб посредством лавинообразного саморазмножения или явного разрушения, то основная функция вирусов типа **«червь»**, действующих в компьютерных сетях, — взлом атакуемой системы.

Червями называют вирусы, которые распространяются по глобальным сетям, поражая целые системы, а не отдельные программы. Это самый коварный вид вирусов, так как объектами нападения в этом случае становятся информационные системы государственного масштаба.

Наиболее опасным червем в середине 2005 г. стала вредоносная программа Kedebe, которая распространяется по электронной почте в виде вложений, замаскированных под якобы секретные документы с информацией о неожиданной смерти Майкла Джексона, поимке Усамы Бен Ладена или аресте автора вируса MyDoom. В тексте таких писем, в частности, указывается, что прикрепленный файл был украден у некой правительственной структуры. В случае если пользователь рискнет просмотреть содержимое документа, червь Kedebe копирует себя на жесткий диск компьютера, регистрируется в ключе автоматического запуска реестра Windows и осуществляет сканирование доступных накопителей в поисках адресов электронной по-

[1] http://protection.net.ru/item/n-ilo-sikou-a-d-n-i-ln-l-l-word

чты. Далее производится массовая рассылка копий вредоносной программы с использованием встроенного SMTP-сервера. Кроме того, Kedebe пытается отключить брандмауэр, деактивировать антивирусное программное обеспечение и проникнуть в файлообменные сети.

Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие и лазерные), а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты, содержащей вирус. Такое заражение может быть и случайным, например, если дискету не вынули из дисковода А и перезагрузили компьютер, при этом дискета может быть и не системной. Заразить дискету гораздо проще. На нее вирус может попасть, даже если дискету просто вставили в дисковод зараженного компьютера и, например, прочитали ее оглавление.

Вирус, как правило, внедряется в рабочую программу таким образом, чтобы при ее запуске управление сначала передалось ему и только после выполнения всех его команд снова вернулось к рабочей программе. Получив доступ к управлению, вирус, прежде всего, переписывает сам себя в другую рабочую программу и заражает ее. После запуска программы, содержащей вирус, становится возможным заражение других файлов. Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXE, COM, SYS, BAT. Крайне редко заражаются текстовые файлы. После заражения программы вирус может осуществить какую-нибудь диверсию, не слишком серьезную, чтобы не привлечь внимания. И, наконец, не забывает возвратить управление той программе, из которой был запущен. Каждое выполнение зараженной программы переносит вирус в следующую. Таким образом, заразится все программное обеспечение.

Для обнаружения вирусов нужно знать признаки их проявления, к которым можно отнести следующие:

- прекращение работы или некорректная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;

- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин.

Компания Sophos, специализирующаяся на вопросах компьютерной безопасности, предупреждают, что в Интернете в ближайшее время может разразиться глобальная вирусная эпидемия[2]. К такому выводу эксперты Sophos пришли, проанализировав код многочисленных вариантов червя Mytob. Модификации Mytob мало чем отличаются друг от друга, и большинство антивирусов способны обнаруживать новые варианты вредоносной программы даже без обновления баз данных. Тем не менее, комментарии в коде Mytob и другие признаки позволяют предположить, что авторы Mytob действуют согласно четкому плану с целью превращения червя в мощный супервирус. В пользу этого говорят и заложенные в тело Mytob функции отключения опций безопасности на инфицированных компьютерах, а также возможность блокирования червем доступа к веб-сайтам антивирусных компаний. Некоторые версии Mytob также способны открывать «черный ход» в систему.

Первая модификация Mytob была обнаружена в конце февраля 2005 г. Вредоносная программа распространяется по электронной почте в виде вложений, а также через дыру в локальной подсистеме аутентификации пользователей (LSASS) операционных систем Microsoft Windows 2000/XP. Попав на компьютер, червь извлекает из файлов с определенными расширениями адреса электронной почты и рассылает по ним свои копии. В настоящее время большая часть вирусного трафика в Интернете приходится именно на долю различных вариантов Mytob. Эксперты опасаются, что очередная модификация этого вируса может принципиально отличаться от предыдущих. Это не позволит быстро блокировать ее распространение и приведет к огромным убыткам.

[2] http://www.sophos.com/virusinfo/articles/mytob.html

5.1.1.2. Шпионские программы

Шпионские программы за последние пять лет стали одной из основных реальных угроз и бед Интернета.

Имеется достаточно много путей инфицирования шпионскими программами. Бороться с ним исключительно сложно. Наиболее часто так называемое «spyware» поставляется в комплекте с популярными бесплатными программами, например, с файлообменными или музыкальными. Во время их установки незаметно инсталлируется дополнительный софт. При этом он может быть упомянут мелким шрифтом в пользовательском соглашении, которое обычно никто не читает[3].

Диапазон действия шпионских программ достаточно широк: они могут записывать все нажатия клавиш на компьютере или вести журнал работы в Интернете с целью маркетингового исследования. Некоторые программы изменяют настройки браузера таким образом, что он автоматически загружает определенные сайты, а самые злостные представители класса «spyware» могут даже вносить изменения в системный реестр, так что их невозможно удалить без профессионального антивируса или специальной программы.

Компьютерные специалисты из Вашингтонского университета разработали программу, которая анализирует сетевой трафик и способна идентифицировать активность четырех самых популярных шпионских программ: Gator, Cydoor, SaveNow и eZula. Программа разрабатывалась с научной целью, чтобы проверить, как много зараженных машин сейчас работают в сети. Ученые проанализировали трафик и определили, что 5,1% всех подключенных компьютеров генерируют этот паразитный трафик. В целом по университету 69% департаментов и офисов имеют в своем составе хотя бы один зараженный компьютер. Всего было исследовано 31 303 компьютера, подключенных к интернету. Результаты работы представлены в журнале New Scientist[4].

При этом нужно учитывать, что университетские пользователи в целом более профессионально обращаются с компьютерами, чем обычные «юзеры». То есть в реальности процент зараженных компьютеров может быть гораздо больше 5%, тем более что шпионских программ тоже гораздо больше, чем четыре. Например, база данных популярного антишпионского дистрибутива Lavasoft Ad-aware содержит

[3] http://www.webplanet.ru/news/security/2004/3/9/spyware.html

[4] http://www.newscientist.com/article.ns?id=dn4745

сигнатуры 9938 шпионских программ (202 семейства в 10 категориях), и эта база пополняется еженедельно.

Некоторые шпионские программы намного коварнее, чем кажутся. Например, Gator и eZula позволяют удаленному администратору не только осуществлять мониторинг, но и запускать на зараженном компьютере программный код.

5.1.1.2.1. Опыт борьбы с Spyware

Бурное развитие шпионского программного обеспечения вынудило начать разработку и принятие ответных мер правового и организационно-технического характера. Рассмотрим некоторые из них. С учетом того, что США — как один из лидеров в ИКТ — раньше других государств почувствовали на себе угрозы от шпионских программ, обратимся к опыту этой страны. Базовым документом США по данной проблеме является Национальная стратегия обеспечения безопасности киберпространства (The national strategy to secure cyberspace). На ее основе в конце 2004 г. в США был одобрен общефедеральный закон, запрещающий spyware и вызвавший волну неприязни со стороны правозащитных организаций по причине узкого толкования spyware и из-за упора на «преднамеренный обман».

Наиболее полным толкованием понятия Spyware отличается закон штата Вашингтон «О шпионском программном обеспечении» (On Regulating Spyware). Закон предусматривает весьма строгие меры наказания за допущенные нарушения[5]. В частности, закон запрещает «обманным способом» изменение стартовой страницы браузера, перенастройку установленного по умолчанию прокси-сервера или подмену провайдера (речь идет, очевидно, о «дайлерах», встречающихся на сайтах «для взрослых») и изменение списка закладок в браузере. Запрещено удаленно менять настройки подключения в Интернет без ведома пользователей. Естественно, запрещен сбор личной информации «преднамеренно обманными способами» и передача их другим лицам, в том числе использование троянов и клавиатурных «жучков».

К числу незаконных деяний также отнесено и обманное препятствование попыткам пользователя деинсталлировать или дезактивировать программное обеспечение (т.е. программы, которые без вашего ведо-

[5] http://www.leg.wa.gov/pub/billinfo/2005-06/Htm/Bills/House%20Passed%20Legislature/1012-S.PL.htm

ма снова устанавливаются на компьютер и активируются снова, этим законом однозначно запрещены). Запрещено и обманное уведомление о том, что та или иная программа дезактивирована, если при этом она продолжает работать. Выведение из строя средств защиты — антивирусов, брандмауэров и антишпионских программ — также запрещается.

Отныне в штате Вашингтон запрещено «открытие многочисленных, последовательных, отдельных рекламных страниц в браузере владельца или оператора компьютера без его, оператора или владельца, разрешения, так, что их невозможно закрыть, не выключая компьютер или закрывая браузер». За принятие этого закона активно ратовала компания Microsoft, занимающаяся, в частности, разработкой антишпионских программ в силу бешеного разгула spyware, пришедшегося на 2004 год.

Обращает на себя внимание, что в плане наказания общефедеральный закон куда строже того, что подписан губернатором штата Вашингтон, поскольку предусматривает не только штраф, но и тюремное заключение сроком до трех лет.

При всей важности правового обеспечения, эксперты небезосновательно полагают, что единственный эффективный способ защитить компьютеры от заражения шпионскими программами — это повышать компьютерную грамотность пользователей, а также проверять систему с помощью специального антишпионского программного обеспечения.

5.1.2. Информационное оружие

Информационная революция, наряду с очевидными благами, которые она уже дала цивилизации, одновременно создает принципиально новые потенциальные угрозы использования ее достижений в целях, несовместимых с задачами поддержания международной стабильности и безопасности, соблюдения принципов отказа от применения силы, невмешательства во внутренние дела государств, уважения прав и свобод человека.

Особая озабоченность возникает в связи с возможностью применения колоссального потенциала ИКТ в интересах обеспечения военно-политического превосходства, силового противоборства, шантажа. Увеличение за счет новейших ИКТ военного потенциала развитых стран ведет к изменению глобального и региональных балансов сил, напряженности между традиционными и нарождающимися центрами силы, появлению новых сфер конфронтации. При этом возникает соблазн воспользоваться обладанием ИКТ для информационной, политической,

экономической, культурной и военной экспансии. К этой деятельности подключаются радикальные политические структуры, «новый» оружейный бизнес, а также террористические и криминальные группировки.

О коварных вариантах применения вирусов, шпионских программ и информационного оружия обычные пользователи, как правило, узнают из специальной литературы или из остросюжетных фильмов. Например, об их внедрении в ИТКС государственного, экономического и военного управления, а также в объекты промышленности, связи, энергетики, транспорта, ЖКХ, уничтожая или парализуя при этом их.

Из кинофильмов многие узнали, как мощные генераторы электромагнитных импульсов разрушают программное обеспечение и уничтожают базы данных даже защищенных информсистем, как искусно сеется паника среди населения и дезинформируется руководство страны.

Указанные полуфантастические киносценарии начинают воплощаться в жизнь. Так, еще в 80-х годах был предан огласке факт о том, что во время американо-иранского кризиса, вызванного захватом американских заложников в Тегеране, США с помощью специальной компьютерной программы заблокировали все зарубежные счета этой страны. Использование средств радиоэлектронной борьбы против Багдада во время карательной операции «Буря в пустыне» дали основание военным специалистам считать Ирак примером первой «информационной Хиросимы», следующими стали Югославия и опять Ирак, где были применены самые изощренные «суперлинки» для информационной войны. Стало известно, что в некоторых странах ведение информационной войны предусматривается военными доктринами и ведется подготовка специальных подразделений, предназначенных для осуществления информационных операций.

В данном контексте заслуживают особого внимания данные главного контрольно-финансового управления Конгресса США, согласно которым сейчас примерно 120 стран мира ведут работы или уже завершили отдельные разработки по развитию возможностей информационно-компьютерного воздействия на информационный ресурс потенциального противника. Для сравнения: разработки в области ядерного оружия ведутся не более чем в 20 странах[6].

---

[6] См. *Крутских А. В.* Война или мир: международные аспекты информационной безопасности // Научные и методологические проблемы информационной безопасности / Под ред. В. П. Шерстюка. М.: МЦНМО, 2004. http://www.cryptography.ru/db/msg.html?mid=1169655

В настоящее время в мире пока не выработано общепринятого определения «информационного оружия», т.к. ИКТ большей своей частью выступают как технологии двойного или вообще невоенного назначения. По мнению экспертов, информационные агрессии могут осуществляться с помощью обычных персональных компьютеров с использованием широких технологических возможностей Интернета.

К характерным чертам информационного оружия можно отнести его универсальность, радикальность воздействия, доступность. Оно отличается широким выбором времени и места применения, сравнительной дешевизной. При этом достаточно сложно определить его национальную принадлежность, т.к. агрессия может осуществляться «чужими руками» или так, что в качестве ответственного за атаку может быть «подставлено» невиновное государство или невинный пользователь Интернета.

Информационное оружие подрывает традиционное понятие государственных границ, используется достаточно скрытно, не нуждается в большой и видимой подготовке. Жертва атаки может даже и не подозревать, что находится под информационным ударом. В силу этого значительно осложняется возможность противодействовать такой агрессии.

Ущерб от применения информационного оружия может быть сопоставим с ОМУ, если оно направлено против военных и гражданских объектов и структур, которые должны функционировать в реальном масштабе времени (системы предупреждения о воздушно-космическом нападении; системы управления ПВО, ПРО, энергетические комплексы, особенно ядерные; промышленные производства).

Информационное оружие трансформирует обычное представление о международном конфликте, т.к. с его помощью можно обойтись без занятия территорий, не иметь дело с военнопленными, уменьшить собственные потери, передать решение боевых задач электронным и беспилотным устройствам.

Информационное оружие, в т.ч. в контексте «гуманитарных интервенций», способно создать вокруг себя некий ореол «гуманности», т.к. формально основывается не на крови, а на электронике. Располагает оно к себе и гражданское общество, ибо его развитие не связано с наращиванием вооруженных сил и даже ведет к их сокращению, т.к. может быть показано в качестве локомотива прогресса (так называемые технологии двойного назначения), а его финансирование можно легко замаскировать в рамках программ развития ИКТ.

Использование ИКТ одним государством против другого вполне может быть квалифицировано как акт информационной войны, если не войны вообще.

Таким образом, время традиционных форм спецпропаганды, «идеологических диверсий» и «подрывных акций» кануло в лету. Информационные технологии повышают их эффективность в неподдающееся вычислению число раз. Разве можно сопоставить, например, радиообращение или печатную листовку с глобально распространяемой информацией через Интернет, мультимедийными материалами, да еще в интерактивном режиме?!

Анализ имевших место конфликтов в Индонезии (Восточный Тимор), Чечне и Югославии показывает, что в них незримо присутствуют «жизненные интересы» некоей «третьей силы» (подробнее в 5.1.3.). Рассмотрим лишь некоторые факты[7].

После референдума о независимости Восточного Тимора общественная организация East Tymor campaign провела с территорий Испании, Португалии и Франции атаку на важные веб-сайты Индонезии, в ходе которой были взломаны ее правительственные сайты, внедрены новейшие компьютерные вирусы для поражения информационных объектов.

Интернет стал еще одним полем боя за так называемую «независимую Ичкерию». Благодаря вэб-сайтам, созданным за пределами России (например, в странах Балтии, Швеции и в Финляндии), всему миру навязывалось видение «реальной» ситуации глазами предводителей «независимой Ичкерии». Напрашивается скорее риторический вопрос, могли ли ваххабисты и аборигены Восточного Тимора организовать столь продвинутые информационные атаки?

Данные факты использования информационного оружия повлияли на позиции большинства стран по проблеме международной информационной безопасности (МИБ), поставленной в ООН Россией. Основу наших оценок составила подготовленная МИД России и согласованная с заинтересованными ведомствами Концепция реализации идеи МИБ, одобренная 21 сентября 1999 г. МВК по информационной безопасности Совбеза России (подробнее в 5.3.).

Большинство экспертов сходятся во мнении, что информационное оружие — в отличие от всех предшествующих видов вооружений — определяется не столько собственными свойствами, сколько харак-

[7] См.: *Смирнов А.И.* Некоторые проблемы информационной безопасности в международных отношениях // Информация. Дипломатия. Психология. — М.: Известия, 2002. С. 346-358.

теристиками объекта, против которого оно применяется. Иными словами, **информационное оружие — это понятие, интегрирующее практически все средства воздействия на основу любого социума — информацию.**

При этом уже трудно сказать, что страшнее для человечества — реальные вирусы сибирской язвы, лихорадки Эбола или виртуальные вирусы — троянские, черви и т.д. Инцидент с достаточно простеньким вирусом «I love you», принесшим многомиллиардный ущерб и глобальную компьютерную панику, убедительно показывает, что человечество подходит к критическому моменту, сопоставимому разве что с моментом принятия в 1968 г. Договора о нераспространении ядерного оружия. В качестве доказательства можно привести факт, что после эпидемии «вируса любви» Пентагон решил ввести шкалу «информационной опасности» Info-Con по аналогии со шкалой состояний военной угрозы.

Применявшаяся во время «холодной войны» система шкала Defence Conditions включала пять состояний: Def-Con Normal — угрозы нет. Далее шли по возрастанию степени боеготовности Def-Con Alpha, Bravo, Charlie и самая высокая — Delta, при которой армия переводится в повышенную боеготовность. Позже аналогичная система была введена для классификации степени террористической угрозы ThreatCon. Шкала была такой же: степень Threat-Con Delta означала, что теракт уже случился либо получены данные о том, что его вероятность очень высока.

Шкала Info-Con тоже состоит из пяти уровней — от нулевого к повышенному. Объявление степеней Info-Con должен исходить из Командного центра U.S. Space Command в Колорадо Спрингз, который отвечает за работу подразделений, занимающихся информационной безопасностью военных сетей (Joint Task Force on Computer Network Defense).

Небезынтересно, что, по данным ABCNews, на самом деле решение о введении шкалы Info-Con было принято еще до эпидемии «вируса любви». Но именно после этой эпидемии военные решили осуществить план по созданию централизованной системы оповещения.

Как и в случае с террористической угрозой, степени информационной опасности определяют меры, которые нужно предпринять при получении такого оповещения. Однако, как подчеркивают военные, есть и существенное отличие. Если во время теракта многие решения принимаются местными военачальниками самостоятельно, то в случае «информационной войны» определяются более централизован-

ные варианты решения проблем, так как речь идет о безопасности распределенных сетей. Ответные меры в данном случае могут быть разные — от блокирования сообщений неизвестных отправителей до отключения целых сетей.

В ходе антитеррористической операции «Возмездие» зафиксировано несколько случаев, подпадавших под шкалы Info-Con. Это было после появления вируса Osama bin Laden, распространявшегося при помощи прикрепленного файла BINLADEN_BRASIL.EXE (gazeta.ru от 24.10.01), а также после взлома веб-сайтов индийских госучреждений пакистанскими хакерами, создавшими виртуальную структуру «Аль-Каида элланс онлайн» (РИАН от 24.10.01).

По имеющейся информации, аналитические центры ряда стран уже ведут проработку сценариев информационных войн, исходя из задачи обеспечения глобального информационного доминирования. Имеют место и провокации. Так, по сообщению lenta.ru (от 22.06.01) со ссылкой на REUTERS, 21 июня 2001 г. перед Конгрессом США выступил представитель неназванной разведывательной службы по имени Лоренс Гершвин, который сообщил, что по агентурным сведениям, Россия и Китай занимаются разработкой компьютерных средств, призванных нанести «долговременный» ущерб США. Он также указал на то, что вскоре можно ожидать появления управляемых компьютерных вирусов, играющих роль супероружия. В это время сами США, как заявил зам.командующего космическими силами (U.S. Space Command) генерал-лейтенант Э.Андерсон, заняты учебными кибервойнами и прочими эмуляциями в рамках создания своей системы электронной защиты.

В 2005 г. вооруженными силами США в рамках сверхсекретной программы по обеспечению безопасности был создан самый крупный в мире отряд программистов-хакеров. Предназначение этого отряда — вести бескровную кибервойну с вражескими сообществами. Правительство Буша потратит миллионы долларов на то, чтобы превратить все существующие средства коммуникаций, включая электрические и телефонные сети, в поля сражений[8].

О создании группы стало известно в ходе прошедших в марте 2005 г. заседаний Комиссии Сената США по делам вооружений. Представители американского военного Стратегического командования (сокращенно Stratcom) обнародовали информацию о существовании этого отряда, получившего обозначение JFCCNW (Joint Functional Component Command for Network Warfare — Совместное

[8] http://www.cnews.ru/newtop/index.shtml?2005/04/28/177780

функциональное командное подразделение для ведения сетевой войны). В соответствии с выполняемыми функциями, его неформально называют отрядом хакеров.

JFCCNW уполномочено обеспечивать безопасность сетей Министерства обороны США. Подразделение также отвечает за проведение сетевых атак и взлом вражеских сетей в рамках программы CNA (Computer Network Attack). Предполагается, что в его состав вошли представители ЦРУ, Агентства национальной безопасности, ФБР.

Дэн Вертон (Den Verton), бывший офицер американской морской разведки, автор книги «Черный лед», предполагает, что созданной команде удастся, разрушив компьютерные сети врагов, проникнуть в их компьютеры с целью захвата и управления стратегически важной информацией. Также группа сможет внедрить саморазмножающийся вирус, который будет способен вывести из строя важнейшие системы противника, в т.ч. ПВО.

Поводом для создания подобного отряда послужила директива, подписанная Президентом США Бушем летом 2002 г. **«Национальная стратегия обеспечения безопасности киберпространства»** (см. Приложение). Согласно этой директиве, правительство США должно было разработать национальную политику по проведению войн в киберпространстве.

Характерно, что разработкой информационного оружия занимаются и такие страны, как КНДР[9]. В случае начала войны с другими странами Северная Корея выставит 600 программистов, которые прошли специальную подготовку для ведения кибервойны, говорится в докладе, представленном южнокорейским оборонным ведомством в парламентский комитет по национальной обороне. Помимо прочего, в их обязанности входит сбор военной разведывательной информации, касающейся таких стран, как США, Южная Корея и Япония, а также осуществление кибератак, сообщает Associated Press.

Основания для опасений у Южной Кореи есть: в июне 2004 года хакеры атаковали серверы парламента и Института оборонного анализа, что дало руководству Южной Кореи основания всерьез задуматься о безопасности страны.

Необходимо отметить, что кибервоины есть практически во всех развитых странах мира. Еще в 2002 г. Ричард Кларк, работавший в ту пору советником по вопросам технологий при администрации США, заявлял, что КНДР, Ирак, Иран, Китай и Россия занимаются подготовкой специалистов по осуществлению кибератак.

[9] http://www.cnews.ru/newtop/index.shtml?2004

По мнению экспертов, специально обученные программисты могут сыграть очень важную роль в современных войнах. К примеру, Китай делает ставку именно на хакеров в случае обострения конфликта с Тайванем. Цель кибератак — максимально осложнить предполагаемое американское вмешательство в возможный конфликт. Речь идет о взломе внутренних сетей, имеющих выход в Интернет, с целью распространения компьютерных вирусов или политических посланий.

По мнению экспертов американского аналитического института Institute for Foreign Policy Analysts, китайские военные рассматривают кибервойну как средство поражения важнейших военных и гражданских компьютерных сетей и делают ставку на стратегию «победы без сражений, с минимальными затратами». Как полагают китайские военные, кибератаки позволят преодолеть военное превосходство США и помогут удержать Вашингтон от вмешательства в военный конфликт между Китаем и Тайванем или же, как минимум, разрушить главные системы противника на ранней стадии войны.

Бразилия стала столицей мирового хакерства и интернет-мошенничества: как заявляют представители федеральной полиции, эта южноамериканская страна является родиной восьми из десяти хакеров, действующих в масштабах всего мира[10].

Такие данные эксперты со всего мира обнародовали на первой международной конференции по борьбе с киберпреступлениями, которая проходила в городе Бразилиа. В работе конференции участвуют более 500 экспертов из разных уголков планеты, общими усилиями пытаясь найти способы эффективной борьбы с электронными преступлениями.

В Бразилии в 2004 г. было совершено 96 тысяч взломов сайтов, что в шесть раз больше, чем в любой другой стране мира. Расцвет киберпреступлений частично связывают со слабым законодательством. Само хакерство в Бразилии не считается преступлением, и чтобы начать расследование, полиция еще должна доказать, что мошенничество действительно имело место. В прошлом году главной целью кибервзломщиков были американские сайты, сообщает BBC.

Большинство хакеров объединяются в группировки с красноречивыми названиями, такими, например, как Breaking Your Security («Взлом вашей защиты») или Virtual Hell («Виртуальный ад»). Многие бразильские хакеры не считают себя преступниками. Они говорят, что взлом сайтов — это в большей степени интеллектуальная игра, а не грабеж.

[10] http://www.cnews.ru/newtop/index.shtml?2004/09/15/163482

В силу этого режим глобального тотального контроля за всеми видами электронной связи и коммуникаций вообще ожесточается с каждым днем.

Достоянием гласности стал проект документа, согласно которому в странах Евросоюза данные обо всех телефонных и других переговорах, а также информация обо всех видах электронной переписки вообще должна будет храниться до одного года[11].

В последней версии проекта директивы, текст которой обнародовала Европейская организация по цифровым правам (European Digital Rights organisation), акцент делается на стандартизации количества, типов и периода времени, в течение которого провайдеры сервисов будут обязаны хранить информацию о телефонных звонках их клиентов, переданных по электронной почте сообщениях, SMS и сообщениях, переданных с помощью сервисов Instant Messaging, а также о других видах электронной передачи данных. «Новинкой» документа можно считать внедрение в систему шпионажа за простыми гражданами технологии определения местоположения телефонного абонента на базе location-based сервисов.

Как сообщает Silicon.com, записи самих телефонных переговоров и текстовых сообщений храниться не будут, однако правоохранительные органы получат доступ к информации об абонентах и их местоположении в момент разговора, времени и продолжительности звонков и т.д.

По мнению Евросоюза, речь идет об «ограниченном ограничении личных свобод» и «ограниченном воздействии на конкурентоспособность отрасли электронной связи» в связи с тем, что европейский телеком вынужден будет хранить огромные массивы информации. Более того, предусмотрены компенсации провайдерам.

Организации по защите гражданских свобод и прав человека встали стеной против законопроекта. В петиции, направленной ими в Евросоюз с призывом отказаться от принятия законопроекта, говорится: «Нигде в Европе не было проведено ни одного исследования, результаты которого подтвердили бы необходимость и важность для целей борьбы с преступностью и терроризмом создания подобной крупномасштабной базы данных, содержащей столь щепетильные сведения».

Аналогичный вердикт вынес в минувшем месяце и Европарламент, заключивший, что необходимо рассмотреть альтернативные предложения по контролю за обменом информацией, предложенные четырь-

[11] http://www.cnews.ru/newtop/index.shtml?2005/08/02/184301

мя другими странами Евросоюза. В отчете Европарламента говорится, что имеются «серьезные сомнения в законности и адекватности предложенных мер», а также подчеркивается, что принятие этого документа «тяжким бременем» ляжет на провайдеров — объем первоначальных вложений, необходимых для реализации подобного рода мер, в расчете на одного оператора составит в среднем 180 млн, а ежегодные затраты — около 50 млн.

Тем временем число спецслужб продолжает множиться и в США. Как сообщает ГИС-Ассоциация[12], там с учетом глобального роста террористической угрозы создан единый оперативный центр (JOIO) Национального агентства геопространственной разведки США (NGA, прежде — NIMA, National Imagery and Mapping agency). Новый центр призван обеспечить более полную интеграцию всех геопространственных разведывательных данных, полученных самыми разными типами сенсоров. В JOIO будут использоваться все наработки специалистов NGA для сбора, обработки и анализа геопространственных данных. Кроме того, центр позволит использовать данные американской службы NSG для выполнения совместных исследований, разработки новых приложений и обеспечения нужд безопасности США.

5.1.3 Информационное противоборство и информационно-психологическая безопасность

С древнейших времен информация являлась важнейшей составляющей любых политически значимых действий. Чем более развитым становился социум, тем более изощренными становились методы получения и распространения разнообразной политической информации и дезинформации, а также политической пропаганды. Сегодня можно с уверенностью говорить об информационных войнах, глобальных информационных противоборствах и локальных конфликтах, которые уже давно не ограничиваются вбрасыванием дезинформации. Стало очевидно, что общество критически зависимо от ИКТ, а наиболее эффективный способ воздействия на противника — воздействие на его граждан с помощью информации.

Считается, что первоначально термин «информационная война» использовал Томас Рона в отчете, подготовленным им в 1976 г. для компании Boeing и названный «Системы оружия и информационная война». Аналитики США начали активно исследовать данное направление. Пик его изучения и апробирования пришелся на период рас-

[12] http://www.gisa.ru

пада СССР и можно без сомнения сказать, что он стал результатом информационной открытости и беззащитности, которые пришли в страну вместе с перестройкой.

Внедрение новейших ИКТ стало катализатором ускорения не только информационных войн, но и таких достаточно латентных процессов, как информационное противоборство, в том числе с информационно-психологической составляющей. В этом контексте необходимо сказать о возможных угрозах конституционным правам и свободам граждан, реализуемым в области духовной жизни и информационной сфере. Здесь же следует упомянуть угрозу системам сбора и хранения данных о личности: медицинская информация, метрические данные, сведения о занятиях и доходах граждан и т.п. Кроме того, в правовом обществе должна обеспечиваться конфиденциальность информации о частной жизни и приватного информационного обмена между частными лицами.

5.1.3.1. Краткая классификация объектов и субъектов информационного противоборства и информационно-психологической деятельности

Наиболее интересными новыми работами в сфере информационного противоборства и информационно-психологической деятельности, на взгляд автора, являются труды А.В.Манойло[13]. Обратимся к ряду его оценок и взглядов на эту актуальную проблему.

Объектом информационного противоборства является любой объект, в отношении которого возможно осуществление информационного воздействия (в том числе и применение информационного оружия) либо иного воздействия (силового, политического, экономического и т. д.), результатом которого будет модификация его свойств как информационной системы.

Общим признаком объекта, который можно рассматривать как объект информационного противоборства, является любая форма использования информации в его функционировании.

Объекты информационного противоборства:

- система социальных отношений информационного общества;

---

[13] *Манойло А. В.* Государственная информационная политика в особых условиях: монография. — М.: Изд. МИФИ, 2003. 388 с., ил.

Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны, монография. — М.: Горячая линия — Телеком, 2003. 541 с., ил.

- система политических отношений информационного общества;
- система психологических отношений информационного общества.

Объектом информационного противоборства может стать любой сегмент информационно-психологического пространства, в том числе:

- массовое и индивидуальное сознание граждан;
- социально-политические системы и процессы;
- информационная инфраструктура;
- информационные и психологические ресурсы.

Под психологическими ресурсами понимаются следующие компоненты:

- система ценностей общества;
- психологическая толерантность системы ценностей (устойчивость системы ценностей по отношению к внешним или внутренним деструктивным воздействиям);
- индивидуальное и массовое сознание граждан;
- психологическая толерантность сознания граждан (устойчивость сознания граждан к манипулятивному воздействию и вовлечению в противоправную деятельность манипулятивными методами тайного принуждения личности);
- психическое здоровье граждан;
- толерантность психического здоровья граждан (устойчивость психического здоровья по отношению к внешним или внутренним деструктивным воздействиям).

Субъекты информационного противоборства:

- государства, их союзы и коалиции;
- международные организации;
- негосударственные незаконные (в том числе — незаконные международные) вооруженные формирования и организации террористической, экстремистской, радикальной политической, радикальной религиозной направленности;
- транснациональные корпорации;
- виртуальные социальные сообщества;
- медиа-корпорации ;
- виртуальные коалиции.

Признаки субъекта информационного противоборства:

- наличие у субъекта в информационно-психологическом пространстве собственных интересов;
- наличие в составе субъекта специальных сил (структур), функционально предназначенных для ведения информационного противоборства или уполномоченных на его ведение;

- обладание и/или разработка информационного оружия, средств его доставки и маскировки;
- под контролем субъекта находится сегмент информационного пространства, в пределах которого он обладает преимущественным правом устанавливать нормы регулирования информационно-психологических отношений (на правах собственности, закрепленных нормами национального и международного законодательства) или государственным суверенитетом;
- существование в официальной идеологии положений, допускающих участие субъекта в информационном противоборстве.

Особую роль в информационной борьбе владельцев открытых информационно-телекоммуникационных сетей (ОИТКС) и разработчиков сетевых технологий — сетевых информационных корпораций и фирм-провайдеров можно охарактеризовать следующим образом.

Контроль за сетевыми ресурсами сосредоточен в руках провайдеров, обеспечивающих доступ в открытые телекоммуникационные сети для других компаний, организаций и частных лиц и гарантирующих стабильность работы с информационными потоками и сетевыми ресурсами. Деятельность провайдеров может подвергаться контролю и давлению как со стороны частных фирм и корпораций, так и органов власти тех государств, на территории которых находятся их сервера, представительства и иные активы. Однако **в тех случаях, когда сетевые ресурсы компании-провайдера находятся на территориях нескольких государств, обеспечивая стабильную работу госорганов власти и других организаций, вмешательство органов власти одного государства в работу такой компании может нанести ущерб политическим и экономическим интересам других государств**. Это обстоятельство, с одной стороны, может привести к нежелательным осложнениям во внешнеполитических отношениях, с другой — становится гарантией безопасности и стабильности для таких компаний, так как в случае нарушения их деятельности на защиту компании придут правительственные структуры и законы тех стран, которые заинтересованы в надежной работе этого канала обмена информацией.

В силу этого можно предположить, что в эвентуальном вооруженном конфликте будут задействованы силы и средства как минимум трех сторон — агрессора, жертвы агрессии и корпораций, обеспечивающих бесперебойное функционирование ОИТКС (являющихся полем деятельности сил для специальных операций государства-агрессора и государства-жертвы) и контролирующих циркулирующую в них информацию. При этом только две из них (агрессор и жертва) находятся в юридически оформленном и закрепленном состоянии войны,

третья же сторона (компания-провайдер) придерживается нейтралитета. **Учитывая, что без участия провайдера, контролирующего ОИТКС, силы для специальных операций обеих сторон вряд ли добьются желаемых результатов, их позиция может стать решающей для обеспечения успешных действий наступающей или обороняющейся стороны.**

Появление надгосударственных информационно-сетевых корпораций, располагающих сетевыми ресурсами, расположенными на территориях различных стран мира, может привести, в случае проведения специальных операций враждующих сторон на каналах ОИТКС и СМИ, к нанесению по вооруженным силам, населению и коммуникациям противника ударов с территорий государств, являющихся нейтральными по отношению к этому конфликту. Внезапность таких ударов будет новым и достаточно важным фактором, способным повлиять на характер боевых действий, и может привести к вовлечению в конфликт новых участников.

При этом особую роль сетевых корпораций в информационно-психологической борьбе государств можно охарактеризовать следующим образом.

1. Транснациональные корпорации в ГИО практически обладают всеми признаками суверенного государства — территорией, определяемой ареалом распространения их сетевой инфраструктуры, стратегическими ресурсами (информационными потоками в их ОИТКС), «населением» — штатом сотрудников и относительно полным суверенитетом.

2. ТНК, разрабатывая новые ИКТ, развивая свои ОИТКС и контролируя циркулирующие по ним потоки, создают театр военных действий, на котором затем будут разворачиваться боевые действия между участниками информационно-психологического противоборства. Итак, можно считать, что информационная война ведется субъектами информационного противоборства в сфере, искусственно создаваемой человеком в результате разработки новых средств воздействия (информационных технологий) и средств доступа к уязвимым объектам нападения (сетевой инфраструктуры), т. е., фактически, в условиях и по законам, определяемым разработчиками и владельцами сетей и технологий.

По прогнозам экспертов развитие, как государств традиционного типа, так и ТНК будет, протекать какое-то время без силовых конфликтов между ними. Традиционная государственность получит свое дальнейшее развитие в тех регионах, где частный бизнес недостаточно развит, чтобы сформировать внутри себя экстерриториальный субъект (сверхкорпорацию). В постиндустриальных регионах (Северная Аме-

рика и Европа) процессы взаимодействия государства и сверхкорпораций будут происходить на базе имеющихся правовых механизмов.

В этих условиях национальные ОИТКС можно рассматривать как один из важнейших факторов информационной геополитики, определяющих геополитический ландшафт в информационно-психологическом пространстве современного общества.

Наиболее остро информационное противоборство проявляется в СМИ и как вид имеет следующие характеристики:

- имеет постоянные интересы в информационном пространстве;
- участвует в формировании ГИО, частично контролирует национальные сегменты информационного пространства и стремится к установлению полного контроля над ними;
- создает в рамках своих структур специальные подразделения или использует национальные структуры, интегрированные в деятельность медиа-корпораций, в функции и задачи которых входит ведение информационного противоборства;
- создает и использует собственный интеллектуальный потенциал и/или использует потенциал национальных структур, интегрированных в деятельность медиа-корпораций, для разработки и испытаний образцов и систем информационного оружия, средств его доставки и маскировки, принципов применения, а также приобретает при необходимости данные средства у третьей стороны;
- разрабатывает и закрепляет на официальном уровне, в том числе в виде нормативных актов, концептуальные и идеологические положения, обосновывающие необходимость участия в информационном противоборстве, определяющие основные принципы и формы участия в нем для данного субъекта.

Появление ЭП имеет значение не только для повышения эффективности управления, но и приводит к изменению роли СМИ и к особой роли в государстве владельцев ОИТКС, обеспечивающих циркуляцию жизненно важных потоков информации.

В сущности, СМИ являются неким промежуточным звеном при прохождении информации от органов и структур госвласти к гражданам. Также предполагается, что роль СМИ в этом процессе должна ограничиваться непосредственной трансляцией той информации, которую они получают из органов госвласти, к отдельным гражданам, что подразумевает полное исключение сознательного искажения, редактирования (цензуры) данной информации, ее тенденциозного освещения и подтасовки фактов. Теоретически это, возможно, однако на практике наблюдается иная картина.

Негосударственные СМИ, принадлежащие различным финансово-промышленным группам, тесно связанным с политической элитой страны, проводят собственную политику оказания воздействия на индивидуальное и массовое сознание гражданского общества в экономических и политических интересах своих владельцев.

Роль СМИ в конкуренции настолько велика, что не случайно практически каждая крупная финансово-промышленная группа в России пытается контролировать (в том числе и на правах полной или частичной собственности) либо телеканал, либо радиостанцию, либо газету, либо и то, и другое, и третье одновременно. Коммерческие СМИ, являясь инструментом достижения собственных целей финансово-промышленной элиты, в этих условиях в принципе не могут быть абсолютно независимыми и абсолютно объективными. В силу этого часть информации о деятельности органов и структур госвласти, поступающая в СМИ, при вещании используется в неполном или искаженном варианте с целью манипулирования общественным мнением, проходит редактирование, компонуется и тенденциозно комментируется в интересах владельцев СМИ. Таким образом, информация о деятельности органов госвласти, проходя через СМИ, нередко сознательно искажается, что может стать серьезным источником угроз безопасности государства.

Внедрение ЭП существенно изменяет роль СМИ в качестве посредника в информационном обмене между властью и населением. ЭП обеспечивает достаточно высокую степень информационной прозрачности деятельности органов госвласти. Не вызывает сомнений, что в информационном обществе СМИ обладают широкими возможностями по манипулированию информацией о деятельности госвласти, что делает их одним из самых опасных противников в информационно-психологической войне. Однако в условиях работы ЭП эти возможности заметно скромнее, а прямой канал связи госвласти с гражданами с использованием ОИТКС дает гражданскому обществу источник получения достоверной информации.

Еще одним видом субъектов информационного противоборства является **виртуальная коалиция.** Она может включать в свой состав любые субъекты информационного противоборства и обладает теми же характеристиками субъектности, что и элементы, в него входящие.

Виртуальные коалиции — это субъекты геополитической конкуренции, характерные для ГИО, в которые могут входить государства, региональные структуры, транснациональные корпорации, медиахолдинги и т.д.

ИКТ позволяют виртуальной коалиции быстро приспосабливаться к изменениям внутренней и внешней геополитической ситуации, маневрировать силами и средствами, быстро восстанавливать свой потенциал после неудач и гибко подбирать для каждого из субъектов адекватные формы участия в соответствии с быстро изменяющимися условиями в современном мире.

В международном контексте проблему информационного противоборства можно проанализировать на примере сообщения «Газета.ru»[14]. В нем говорится, что Вашингтон начинает масштабную кампанию по улучшению своего образа за границей. Согласно источникам агентства Reuters в военном ведомстве США, сейчас администрация изучает программу соответствующих мероприятий. Америка возвращается к методам пропаганды и контрпропаганды времен холодной войны. В Пентагоне, Белом доме и госдепартаменте США спорят как о методах информационной войны, так и о возможных объектах воздействия. Наиболее радикальные планы (их высказывает руководство Пентагона) предполагают информационную обработку в том числе и союзников США, таких, как, например, Пакистан и Германия. Но главными объектами информационной войны США считают страны Ближнего Востока, а также те европейские государства, где существуют центры исламского экстремизма.

По словам источников в Пентагоне, власти пока не могут определиться с масштабом и методами реформы по улучшению имиджа. Военное командование, например, обеспокоено размыванием границ между использованием дезинформации и предоставлением достоверных фактов другим странам. По мнению сторонников агрессивного пиара, незначительное вранье только на пользу США.

Эти военные приводят в пример случай, когда в репортаже CNN прошла заведомая дезинформация. Американский военный объявил в эфире о начале наступления американских войск на город Эль-Фаллуджа в Ираке. В результате, говорят сторонники реформы, иракские партизаны обнаружили себя и слабые места в своей обороне. Есть и другое мнение. Согласно ему, заведомая ложь в эфире CNN дискредитировала и телеканал, и Пентагон, а значит, принесла больше вреда, чем пользы.

По сведениям New York Times, власти США намерены сделать информационную войну государственным приоритетом. Согласно некоторым источникам, в руководстве Пентагона обсуждается возможность возрождения так называемого **отдела по стратегическому влиянию**.

[14] 14.12.2004 11:07

Это подразделение в рамках минобороны было сформировано вскоре после терактов 11 сентября 2001 г. и просуществовало до февраля 2002 г., то есть менее полугода. Подразделение занималось внешнеполитическим пиаром и должно было оказывать влияние на общественное мнение о США в странах исламского мира. Однако тогда власти сочли, что подразделение со своей задачей не справилось.

Ожидается, что в Пентагоне возродится если не сам отдел по стратегическому влиянию, то, по крайней мере, его методы. При этом Вашингтон увеличит расходы на противодействие антиамериканским настроениям в мире, прежде всего в мусульманских и арабских странах. Согласно источникам, возможно восстановление ряда закрытых программ отдела по стратегическому влиянию. Следует ждать, например, возобновления информационной войны в Интернете. Эксперты Пентагона будут дискредитировать мечети, проповедующие антиамериканизм, на специальных интернет-сайтах и в прессе. Планируется также переводить на арабский язык больше западной литературы и создавать американские информцентры в мусульманских странах.

Полузабытые методы холодной войны Вашингтон планирует противопоставить в том числе и пиару, проводимому террористами, которые, чаще всего в целях устрашения, распространяют через телевидение и Интернет заведомую ложь (см.5.3.2.).

5.2. Базовые подходы России к проблеме информационной безопасности

Под воздействием информационной глобализации вся система мироустройства претерпевает кардинальные структурные изменения. На авансцену международной жизни выходят наднациональные структуры, интересы которых по ряду вопросов вступают во взаимные противоречия, противопоставляются интересам отдельных государств. Резко обострилась угроза международного терроризма.

До недавнего времени под национальной безопасностью понималось сохранение суверенитета и территориальной целостности государства, его устойчивость перед угрозой применения вооруженной силы со стороны других субъектов международных отношений. Однако вызовы последнего десятилетия потребовали иных подходов к оценке содержания национальной безопасности. Сегодня национальная безопасность видится как комплексная системная проблема. Она должна рассматриваться в более широком контексте и учитывать наличие многообразных факторов и угроз, а не только угрозы

военного нападения, захвата территории и физического уничтожения населения.

Подходы России к проблеме безопасности отражены не только в Концепции национальной безопасности, но и практически во всех основополагающих документах внутренней и внешней политики.

В совокупности эти документы образуют взаимоувязанную систему взглядов на обеспечение национальной безопасности страны. Эта работа ведется непрерывно. Перечень базовых документов постоянно наращивается. Начиная с 1999 г. разработаны: Доктрина информационной безопасности, Концепция внешней политики, Государственная стратегия экономической безопасности, Основы политики Российской Федерации в области развития оборонно-промышленного комплекса, в области развития науки и технологий, Основы военно-технической политики, Основы государственной политики в ряде таких важнейших областей деятельности государства, как морская, авиационная и космическая и др. Завершена или близится к завершению работа по подготовке концептуальных документов в сфере промышленной, научно-технологической и инновационной, химической и биологической безопасности, а также в области обеспечения защищенности особо опасных и критически важных объектов инфраструктуры государства и населения страны. Продолжается работа по развитию и углублению отдельных положений Доктрины информационной безопасности, поскольку одним из наиболее важных факторов, определяющих развитие современного общества, является продолжающаяся «информационная революция»[15].

Интенсивное совершенствование ИКТ и динамичное развитие на их основе глобальной и национальных информационных инфраструктур является одной из характерных примет нашего времени. Во многом благодаря воздействию этого фактора начали складываться условия для постепенного перехода человечества к постиндустриальной фазе своего развития. **Одним из наиболее важных признаков этого общества является изменение предмета и орудий труда большей части людей. Предметом их труда становятся информация и знания, а орудием труда — информационные технологии.**

Изменения в общественных отношениях затрагивают, прежде всего, производственную сферу, которая в значительной степени сори-

[15] http://www.cryptography.ru/db/msg.html?mid=1169588; *В. П. Шерстюк*. Проблемы информационной безопасности в современном мире // Доклад на конференции «Математика и безопасность информационных технологий» (МаБИТ*-03, МГУ, 23—24 октября 2003 г.)*

ентирована на производство продуктов информационной и интеллектуальной деятельности, совершенствование ИКТ, оказание услуг в создании новой информации и новых знаний. Связанные с этим изменения условий человеческой деятельности неминуемо затрагивают и духовную, и социальную сферу жизни общества.

В то же время переход цивилизации в фазу постиндустриального развития своей обратной стороной имеет объективное усиление зависимости общества от нормального функционирования глобальной и национальных информационных инфраструктур. Очевидно, что «вхождение» тех или иных государств в ГИО не отменяет наличия у них национальных интересов, в том числе в информационной сфере, и необходимости обеспечения безопасности этих интересов от угрозы ущемления со стороны других государств, а также таких опасных субъектов современной жизни, как международные террористические организации.

Стремительное развитие ИКТ привело к формированию фундаментальной зависимости критически важных национальных инфраструктур России от этих технологий и обусловило возникновение принципиально новых угроз. Эти угрозы связаны, прежде всего, с возможностью использования ИКТ в целях, несовместимых с задачами поддержания международной стабильности и безопасности, соблюдения принципов отказа от применения силы, невмешательства во внутренние дела государств, уважения прав и свобод человека.

Особую озабоченность в этом плане вызывает возможность разработки, применения и распространения информационного оружия и возникающая угроза информационных войн и информационного терроризма, способных вызвать конфликты, разрушительные последствия которых могут быть сопоставимы с последствиями применения оружия массового уничтожения.

5.2.1. Доктрина информационной безопасности России — ответ на новые вызовы и угрозы в информационной сфере

В Доктрине информационной безопасности России, утвержденной Указом Президента России 9 сентября 2000 г., отмечается, что информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности России[16]. При этом подчеркнуто, что национальная безопасность Рос-

[16] http://www.ln.mid.ru/ns-osndoc.nsf/0e9272befa34209743256c630042d1aa/4db2749a4b55f02f432569fb004872a4?OpenDocument

сии существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать. Данный постулат вытекает из духа и буквы Окинавской хартии глобального информационного общества (см. подробнее в главе 3).

В доктрине **под информационной безопасностью России понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства**.

Интересы личности в информсфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информсфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информсфере заключаются в создании условий для гармоничного развития информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов в информсфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Как уже отмечалось, в доктрине выделены следующие **четыре основные составляющие национальных интересов в информационной сфере**.

Первая включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая включает в себя информационное обеспечение госполитики, связанное с доведением до российской и международной общественности достоверной информации о госполитике, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым госинформресурсам.

Третья включает в себя развитие современных ИКТ, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия призвана занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности телекоммуникации и связи.

Четвертая включает в себя защиту информресурсов от несанкционированного доступа, обеспечение безопасности ИТКС, как развернутых, так и создаваемых в России.

В доктрине к наиболее важным объектам обеспечения информационной безопасности России **в сфере внешней политики** отнесены:

- информресурсы федеральных органов исполнительной власти, реализующих внешнюю политику, российских представительств и организаций за рубежом, представительств России при международных организациях;
- информресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику России на территориях субъектов Федерации;
- информресурсы российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующих внешнюю политику России;
- блокирование деятельности российских СМИ по разъяснению зарубежной аудитории целей и основных направлений госполитики России, ее мнения по социально значимым событиям российской и международной жизни.

Из внешних угроз информбезопасности России в сфере внешней политики наибольшую опасность представляют:

- информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики России;

- распространение за рубежом дезинформации о внешней политике России;
- нарушение прав российских граждан и юридических лиц в информсфере за рубежом;
- попытки несанкционированного доступа к информации и воздействия на информресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику России, представительств и организаций за рубежом, представительств при международных организациях.

Из внутренних угроз информбезопасности России в сфере внешней политики наибольшую опасность представляют:

- нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику России, и на подведомственных им предприятиях, в учреждениях и организациях;
- информационно-пропагандистская деятельность политических сил, общественных объединений, СМИ и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности России;
- недостаточная информированность населения о внешнеполитической деятельности России.

Основными мероприятиями по обеспечению информбезопасности в сфере внешней политики являются:

- разработка основных направлений госполитики в области совершенствования информобеспечения внешнеполитического курса;
- разработка и реализация комплекса мер по усилению информбезопасности информационной инфраструктуры федеральных органов исполнительной власти, реализующих внешнюю политику, российских представительств и организаций за рубежом, представительств при международных организациях;
- создание российским представительствам и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике России;
- совершенствование информобеспечения работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом;
- совершенствование информобеспечения субъектов Федерации по вопросам внешнеполитической деятельности, которые входят в их компетенцию.

5.2.1.1. Международное сотрудничество России по обеспечению информационной безопасности

В Доктрине отмечено, что особенность международного сотрудничества России в области обеспечения информбезопасности состоит в том, что оно осуществляется в условиях обострения международной конкуренции за обладание технологическими и информресурсами, за доминирование на рынках сбыта. Это происходит в условиях продолжения попыток создания структуры международных отношений, основанной на односторонних решениях ключевых проблем мировой политики, противодействия укреплению роли России как одного из влиятельных центров формирующегося многополярного мира, усиления технологического отрыва ведущих держав мира и наращивания их возможностей для создания информационного оружия.

Все это может привести к новому этапу развертывания гонки вооружений в информсфере, нарастанию угрозы агентурного и оперативно-технического проникновения в Россию иностранных разведок, в том числе с использованием глобальной инфраструктуры Интернет.

Основными направлениями международного сотрудничества России в области обеспечения информбезопасности определены:

- запрещение разработки, распространения и применения информационного оружия;
- обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;
- координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;
- предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информобеспечения мировой торговли, к информации правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

При осуществлении международного сотрудничества России в области обеспечения информбезопасности особое внимание уделяется проблемам взаимодействия с государствами — участниками СНГ.

Для осуществления этого сотрудничества по указанным основным направлениям необходимо активное участие России во всех международных организациях, осуществляющих деятельность в области информбезопасности, в том числе в сфере стандартизации и сертификации средств информатизации и защиты информации.

Наряду с уже ранее рассмотренными аспектами участия России в данной деятельности, в следующем параграфе пойдет речь о разработке и продвижении Россией концепции международной информационной безопасности.

Чрезвычайно важным компонентом развития положений Доктрины и их практической конкретизации стали всероссийские конференции по информбезопасности, которые приобрели особую популярность на веб-сайте «Инфофорум». Так, на конференции в сентябре 2004 г. было подчеркнуто, что кризисные ситуации в информпространстве России, как правило, являются последствиями разного рода воздействий на ИТКС, в результате которых становится невозможным доступ к информресурсам, искажается информация, нарушаются права собственности на информацию или правила ознакомления с информацией, содержащей сведения, составляющие гостайну, или сведения ограниченного доступа[17].

Естественно, что не всякое такое нарушение приводит к чрезвычайной ситуации. Так, заражение компьютерным вирусом одного домашнего персонального компьютера, на котором отсутствует уникальная информация, не приводит к чрезвычайной ситуации. Однако широкомасштабная вирусная атака, проводимая сетевым компьютерным DOS-вирусом, в результате которой выходят из строя целые сегменты компьютерной сети, приводит к чрезвычайной ситуации в информпространстве.

Угрозы в информпространстве обусловлены как объективными, так и субъективными факторами. К объективным факторам следует отнести последствия стихийных бедствий, экологических или техногенных катастроф. К субъективным факторам относятся преднамеренные или непреднамеренные действия участников информобмена, приводящие к возникновению чрезвычайных ситуаций, а также ошибки и недостатки при проектировании, создании и эксплуатации ИТКС, обусловленные недостатком квалификации разработчиков или отсутствием необходимых финансовых средств у их заказчиков.

---

[17] См.: *Кузьмин А.С.*, д.ф.-м.н., профессор, член-корр. Академии криптографии, начальник Управления Центра безопасности связи ФСБ России// Основные угрозы безопасности Российской Федерации в информационной сфере.

Следует подчеркнуть, что **особенностью стратегических рисков в информационном пространстве является доминирование субъективного фактора возникновения чрезвычайных ситуаций над объективным фактором. Роль субъективного фактора еще более возросла с появлением компьютерного терроризма (или кибертерроризма).**

Среди проявлений субъективного фактора следует особо выделить компьютерные вирусы, в том числе троянские программы, сетевые черви, логические бомбы. Так, по оценкам экспертов, 2 из 3 электронных послания содержат «спам», каждое 208 послание содержит вирус, каждый день в среднем обнаруживается около 20 новых вирусов.

Угрозы безопасности информпространства побуждают к разработке комплекса мероприятий, направленных на снижение риска возникновения чрезвычайной ситуации. Для этого необходимо прежде всего определить совокупность угроз применительно к конкретному сегменту информпространства и допустимый уровень риска их реализации и оценить затраты на локализацию и ликвидацию последствий.

Наиболее сложной задачей является оценка величины вероятности реализации той или иной угрозы, а также тенденций изменения угроз при тех или иных условиях и появление новых угроз, обусловленных развитием ИКТ. Так, развитие глобальной сети Интернет сделало реальностью угрозу вычислительного терроризма, заключающуюся в негласном использовании громадных вычислительных ресурсов сети Интернет для взлома информсистем.

Основой для проведения мероприятий по предотвращению чрезвычайных ситуаций является всесторонний анализ угроз применительно к конкретному сегменту информпространства. Важной составляющей этого анализа является определение механизмов и достаточных средств защиты для снижения рисков до приемлемого уровня. При этом должен соблюдаться принцип «разумной достаточности» с тем, чтобы использование средств защиты ИТКС не снижало оперативность обработки и передачи информации. Следует также отметить, что эффективное предупреждение чрезвычайных ситуаций в информпространстве России возможно только на основе комплексного, системного подхода к решению этой проблемы.

Важнейшим механизмом повышения безопасности информпространства является государственно-правовое регулирование деятельности субъектов информобмена и рынка информуслуг. Примерами подобных законодательных актов являются Закон Российской Федерации «Об информации, информатизации и защите информации», Федеральный

Закон «Об участии в международном информационном обмене», а также ряд Указов Президента Российской Федерации.

Для повышения надежности информсистем, снижения риска злонамеренного использования недокументированных возможностей, обусловленных сложностью ИКТ, целесообразно опираться на отечественные разработки, выполненные в рамках действующей в стране системы оценки качества продукции, что позволяет обеспечить необходимый уровень их защищенности.

В России накоплен значительный опыт разработки защищенных информсистем, причем не только государственных и не только закрытых. Разработаны и успешно применяются криптографические и системно-технические методы защиты ИКТ, в том числе Интернет-технологий. Имеется значительное число сертифицированных средств защиты информации. Все это позволяет создавать полнофункциональные системы защиты информресурсов. При этом следует иметь в виду, что за состоянием защищенности информации должен осуществляться постоянный контроль, а сами средства защиты должны постоянно совершенствоваться ввиду развития методов и средств нападения на информресурсы.

Поэтому одним из главных компонентов системы обеспечения безопасности киберпространства России должен стать постоянный мониторинг уровня защищенности сегментов ее информпространства, а также создание служб по ликвидации последствий чрезвычайных ситуаций в информсфере. На основании результатов мониторинга можно заранее выявлять уязвимые места в инфраструктуре и принимать упреждающие меры по недопущению чрезвычайных ситуаций, в частности, путем организации антивирусной защиты ИТКС. В этом направлении уже сделаны определенные шаги. В ФСБ России начал функционировать Антивирусный центр, главными задачами которого являются оценка качества антивирусных средств и обновлений к ним, выработка рекомендаций по построению антивирусной защиты ИТКС органов госвласти России, оказание помощи при ликвидации последствий заражений, оценки уровня защищенности систем.

Учитывая высокую сложность таких работ, а также взаимное влияние на уровень защищенности ИТКС органов госвласти, коммерческих структур и компьютеров частных лиц, функционирующих в едином информпространстве России, актуальным является вопрос о координации деятельности уполномоченных госорганов и центров доверия для выработки общих подходов к оценке реального уровня защищенности и рекомендаций по устранению слабостей в защите информсистем.

Важным для обеспечения безопасности информресурсов является и повышение уровня образования пользователей в области информатики, повышение квалификации разработчиков, экспертов и обслуживающего персонала ИТКС. В России сложилась достаточно эффективная система подготовки и переподготовки специалистов в области информбезопасности. Учебно-методическое объединение по этой специальности, возглавляемое ИКСИ Академии ФСБ, объединяет более 75 вузов России.

Проблемы, связанные с повышением безопасности информсферы, являются сложными, многоплановыми и взаимосвязанными. Они требуют постоянного, неослабевающего внимания со стороны государства и общества. Развитие ИКТ побуждает к постоянному приложению совместных усилий по совершенствованию методов и средств, позволяющих достоверно оценивать угрозы безопасности информсферы и адекватно реагировать на них.

По мнению экспертов, социальные интересы человека, которые необходимо охранять в информационном обществе, заключаются прежде всего в реальном обеспечении прав и свобод человека на доступ к открытой информации, на использование информации в интересах осуществления не запрещенной законом деятельности, а также в защите информации, обеспечивающей личную безопасность, духовное и интеллектуальное развитие. Наиболее опасным источником угроз этим интересам является существенное расширение возможности манипулирования сознанием человека за счет формирования вокруг него индивидуального «виртуального информационного пространства», а также возможности использования технологий воздействия на его психическую деятельность. Сложность процедур, реализуемых в современных технологиях, критически увеличивает зависимость человека от других людей, осуществляющих разработку ИКТ, определение алгоритмов поиска требуемой информации, ее предварительной обработки, приведения к виду, удобному для восприятия, доведение до потребителя. По существу, данные люди во многом формируют для человека информационный фон его жизни. Они определяют «информационные» условия его жизни и деятельности. Именно поэтому представляется исключительно важным обеспечить безопасность взаимодействия человека с информационной инфраструктурой.

Другим опасным источником угроз социальным интересам человека является неправомерное использование персональных данных, накапливаемых различными структурами, в том числе органами государственной власти, а также расширение возможностей скрытого сбора информации, составляющей его личную и семейную тайну, све-

дений о его частной жизни. Это обусловлено дальнейшими успехами в области миниатюризации средств скрытого сбора и передачи информации. Для противодействия угрозам социальным интересам человека необходимо разработать и реализовать действенные правовые механизмы охраны этих сведений.

Интересы общества в информационной сфере заключаются в обеспечении социальной стабильности и экономического процветания на базе упрочения демократии, поддержания общественного согласия и повышения созидательной активности населения. Одним из источников угроз интересам общества в информационной сфере является непрерывное усложнение информационных и телекоммуникационных систем, сетей связи, информационной составляющей критически важных объектов инфраструктуры жизни общества. Эти угрозы могут проявляться в виде нарушения устойчивости функционирования составляющих информационной инфраструктуры, несанкционированного доступа к охраняемой законом информации экономически и социально значимых структур со стороны преступных, в том числе террористических, организаций. Объектами реализации таких угроз могут выступать информационные системы энергетической, транспортной и некоторых других инфраструктур. Потенциал так называемой «киберпреступности» весьма высок. По имеющимся данным, только за последние три года общее количество зарегистрированных преступлений в сфере компьютерных технологий возросло в России более чем в 150 раз. Тенденция роста этого вида преступлений отмечается и в других странах.

Масштаб возможных последствий нарушения работоспособности технического и программного обеспечения информационных систем можно представить по затратам на решение «Проблемы-2000». По некоторым оценкам, мировое сообщество затратило на эти цели около 500 млрд долл. США.

Интересы государства в информсфере заключаются в использовании информации и информационной инфраструктуры для обеспечения суверенитета и территориальной целостности страны, разъяснения населению страны и международной общественности содержания и направленности государственной политики, в создании условий для гармоничного развития информационной инфраструктуры, в безусловном исполнении законодательства, в поддержании правопорядка, в развитии международного сотрудничества на основе партнерства. Наиболее опасными источниками угроз интересам государства в информационной сфере являются неконтролируемое распространение «информационного оружия» и развер-

тывание гонки вооружений в этой области, попытки реализации концепций ведения «информационных войн». Это обстоятельство особенно опасно в условиях существования почти монопольного положения компаний небольшого количества стран на рынке информационных продуктов, так как способно спровоцировать желание использовать имеющееся превосходство для достижения тех или иных политических целей. Данные угрозы могут проявляться также в виде получения противоправного доступа к сведениям, составляющим государственную тайну, к другой конфиденциальной информации, раскрытие которой может нанести ущерб интересам государства.

В итоговых документах Всемирной встречи по ГИО в Женеве (декабрь, 2003 г.) определены основные принципы и направления сотрудничества в области формирования условий для перехода цивилизации к постиндустриальной фазе развития на значительную перспективу (см. Приложение). Основным их назначением должно стать противодействие угрозам использования информационной инфраструктуры в целях, несовместимых с Уставом ООН, и, прежде всего, угрозам:

- манипулирования поведением человека;
- нарушения устойчивости функционирования составляющих информационной инфраструктуры, несанкционированного доступа к охраняемой законом информации со стороны преступных, в том числе террористических, организаций;
- использования «информационного оружия», создаваемого на базе современных информационных технологий, и развертывание гонки вооружений в этой области, реализации концепций ведения «информационных войн».

Бурное развитие ИКТ неизбежно оказывает влияние и на формирование внутренней политики государства, что требует постоянной адаптации существующих государственных и общественных институтов к этим инновациям. Содержание государственной информационной политики требует своей глубокой и комплексной проработки. Под воздействием общемирового интенсивного развития ИКТ заинтересованные органы госвласти с участием ученых и специалистов призваны активно разрабатывать и внедрять концептуальные и программные основы, принципы, а также практические приложения в этой области.

Успешность противодействия угрозам в информационной сфере во многом зависит от того, насколько эффективно будет использован потенциал, который накоплен российской наукой в

области решения научно-технических проблем информационной безопасности и, прежде всего, математических проблем обеспечения безопасности информационных технологий. Полагаю, что свою лепту в становление России как информационной державы внесет недавно созданный в системе Московского государственного университета Институт проблем информационной безопасности.

Феномен информационной революции оказывает все большее влияние не только на социум, но и на международные отношения.

В этом контексте наиболее существенными являются такие характерные черты ИКТ, как: трансграничность, способность проникать сквозь традиционные межгосударственные барьеры и вытекающая отсюда глобальность охвата ими различных сфер деятельности человеческого общества.

В Концепции внешней политики России отмечается[18] важность доведения до широких кругов мировой общественности объективной и точной информации о ее позициях по основным международным проблемам, внешнеполитических инициативах и действиях России, а также о достижениях российской культуры, науки, интеллектуального творчества. На передний план выдвигается задача формирования за рубежом позитивного восприятия России, дружественного отношения к ней. Неотъемлемым элементом соответствующей работы должны стать целенаправленные усилия по широкому разъяснению за рубежом сути внутренней политики России, происходящих в стране процессов. Актуальным становится ускоренное развитие собственных эффективных средств информационного влияния на общественное мнение за рубежом.

5.3.Инициативы России по международной информационной безопасности

Прямое политическое следствие информационной революции — ускорение процесса трансформации международных отношений, идущее по многим направлениям[19].

---

[18] http://www.ln.mid.ru/ns-osndoc.nsf/0e9272befa34209743256c630042d1aa/fd86620b371b0cf7432569fb004872a7?OpenDocument

[19] См. Крутских А.В., Крамаренко Г.И. Дипломатия и информационно-коммуникационная революция. Международная жизнь. 2003.№7.

С учетом того, что новые ИКТ услуги и виды деятельности все менее подконтрольны федеральным правительствам, размывается традиционная концепция национального суверенитета. Кроме того, регулирование международным правом отношений в сфере ИКТ между самими государствами серьезно отстает от практики их применения.

С точки зрения внешней политики, важнейшая особенность ИКТ — это использование двойных технологий. Принципиально иной в связи с этим становится проблема обеспечения национальной и международной безопасности, так как вся совокупность ИКТ ресурсов страны становится одновременно и объектом враждебного воздействия, и информационным оружием.

В силу этого возникает угроза применения потенциала ИКТ в интересах обеспечения военно-политического превосходства и шантажа на международной арене. При этом рост военного потенциала за счет новейших ИКТ ведет к изменению глобального и регионального балансов сил, напряженности между традиционными и нарождающимися центрами силы, появлению новых сфер конфронтации. Новое содержание получает понятие агрессии.

ИКТ способствовали образованию межгосударственных альянсов в самой структуре международных отношений по признаку информационно-коммуникационных интересов. Основой деятельности таких объединений является обеспечение единого доступа к определенной ИКТ и проведение единой инфокоммуникационной политики. Практически, они играют роль картелей и неких политических союзов вокруг новых технологий, например, сфере навигации — на базе американской GPS, западноевропейской ГАЛИЛЕО, российской ГЛОНАСС или региональных международных телекоммуникационных организаций.

Как известно, в связи с освоением космического пространства произошла революция в телекоммуникационной сфере. В этот период были подписаны межправительственные соглашения о создании целого ряда международных организаций, предоставляющих услуги спутниковой связи для различных целей (коммерческая связь для морских и воздушных судов, спутниковая связь для обеспечения безопасности жизнедеятельности на море, теле- и радиовещание, передача данных и т.п.): «Интелсат», «Инмарсат», «Евтелсат», «Интерспутник», а также об учреждении гуманитарной Международной программы КОСПАС — САРСАТ.

МИД России совместно с Минсвязи России и Минтрансом России участвовал в переговорах, в работе над межправительственными

соглашениями и в их последующей ратификации, в решении политически значимых вопросов.

Как уже отмечалось в третьей главе, в 1993 г. США выдвинули инициативу создания национального информационного общества, а уже в марте 1994 г. на Всемирной конференции по электросвязи в Буэнос-Айресе вице-президент США А.Гор представил идею создания глобальной информационной инфраструктуры. В феврале 1995 г. лидеры «семерки» на конференции в Брюсселе призвали объединить финансовые, материальные и человеческие ресурсы всего мирового сообщества для создания ГИО. В мае 1996 г. в Мидранде (ЮАР) состоялась межправительственная конференция «Информационное общество и развитие» с участием наряду с государствами «семерки» России, Австралии, Израиля и 30 развивающихся стран, включая Китай и Индию. С тех пор Россия постоянно участвует во всех значимых мероприятиях по проблематике ГИО.

Данная проблематика включалась в повестку дня встреч «восьмерки» на высшем уровне в Галифаксе (1995 г., когда Россия впервые приняла участие в этих встречах), Лионе (1996 г.), на Окинаве (2000 г.), в Генуе (2001 г.), в Кананаскисе (2002 г.). Представители России участвовали во всех этапах подготовки их проведения и реализации принятых решений.

Особое внимание при этом уделялось проблеме информационной безопасности, поскольку международное сотрудничество России в данной области — неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое сообщество. Такое сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества, включая России.

5.3.1. Разработка концепции международной информационной безопасности

Осознание того факта, что появление и распространение информационного оружия, милитаризация ИКТ явятся мощным дестабилизирующим фактором международных отношений, а также стремление выйти из губительного цикла гонки новых технологических вооружений и перевести процессы гражданской и военной информатизации в плоскость международно-правового регулирования, побудили Россию взять на себя инициативу в ООН по официальной по-

становке вопроса об обеспечении международной информационной безопасности.

Первым шагом на этом направлении стала попытка убедить США в том, что ИКТ могут иметь существенную негативную оборотную сторону и, следовательно, не должны развиваться самотеком без адекватного международного контроля. В принятом в сентябре 1998 г. на встрече президентов России и США совместном Заявлении «Об общих вызовах безопасности на рубеже XXI века» зафиксировано согласие активизировать совместные усилия по противодействию транснациональным угрозам экономике и безопасности, включая преступления с использованием компьютерной техники и других высоких технологий.

В дальнейшем, на уровне дипломатических экспертов США заняли явно выжидательную позицию, выделяя в качестве приоритетных для себя лишь криминальные и террористические аспекты проблемы и затушевывая ее военную составляющую.

Учитывая масштабы глобального информационного вызова, невозможность его решения усилиями одной или нескольких стран — в силу неделимости мирового информпространства, если, конечно, не обрекать себя на самоизоляцию, — Россия сосредоточила активные действия в ООН.

В целях создания международно-правового режима по обеспечению информационной безопасности Межведомственная комиссия по информационной безопасности Совета Безопасности России в 1998 г. одобрила Концепцию реализации идеи международной информационной безопасности (МИБ), разработанную МИД России во взаимодействии с заинтересованными федеральными органами исполнительной власти.

В соответствии с ней в адрес Генерального секретаря ООН было направлено специальное Послание по проблеме МИБ министра иностранных дел России И.С. Иванова. Особый акцент в нем был сделан на необходимости предотвращения появления принципиально новой — информационной — сферы конфронтации и развязывания принципиально новых военных конфликтов. Практическим развитием этой российской инициативы стало внесение в ходе 53-й сессии ГА ООН разработанного МИД совместно с ключевыми ведомствами проекта резолюции под названием «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», консенсусом принятый 4 декабря 1998 г.

5.3.2. Продвижение концепции МИБ

Резолюция (A/RES/53/70) предложила государствам — членам ООН продолжить обсуждение вопросов информационной безопасности, дать конкретные определения угроз, предложить свои оценки проблемы, включая разработку международных принципов обеспечения безопасности глобальных информационных систем. О таких оценках страны-члены должны информировать Генерального секретаря ООН, которому поручено представить соответствующий доклад на следующей сессии Генассамблеи ООН. Оценки России были переданы Генсекретарю ООН в июне 1999 г.

Построение МИБ (из документа A/54/213, внесенного Россией в ООН 9 июня 1999 г.):

a) определение признаков и классификация информационных войн;

b) определение признаков и классификация информационного оружия, а также методов и средств, которые можно отнести к информационному оружию;

c) ограничение оборота информационного оружия;

d) запрещение разработки, распространения и применения особо опасных видов информационного оружия;

e) предотвращение угрозы возникновения информационных войн;

f) запрещение использования информационных технологий и средств во враждебных целях и, в частности, против согласованных категорий объектов;

g) признание сравнимости применения информационного оружия в отношении критически важных структур с последствиями применения оружия массового поражения;

h) создание условий равноправного и безопасного международного информационного обмена на основе баланса интересов личности, общества и государства;

i) предотвращение угроз использования информационных технологий и средств в террористических и других преступных целях;

j) предотвращение угрозы использования информационных технологий и средств для воздействия на общественное сознание с целью дестабилизации общества и государства;

k) разработка процедуры взаимного уведомления и предотвращения трансграничного несанкционированного информационного воздействия;

l) создание механизма разрешения конфликтных ситуаций в сфере информационной безопасности;

m) создание международной системы сертификации технологий и средств информатизации (в том числе программно-технических) в части гарантий их информационной безопасности;

n) развитие системы международного взаимодействия правоохранительных органов по предотвращению преступлений в информационной сфере;

o) создание механизма контроля за выполнением условий режима международной информационной безопасности;

p) гармонизация национальных законодательств в части обеспечения информационной безопасности.

Резолюция 53/70 положила начало обсуждению создания нового международно-правового режима. В соответствии с ее рекомендациями Институтом ООН по проблемам разоружения (ЮНИДИР) и Департаментом по вопросам разоружения Секретариата ООН в августе 1999 г. в Женеве был организован международный семинар по вопросам МИБ. Задача семинара заключалась в выявлении подходов различных стран в связи с продолжением дискуссии по этой теме на 54-й сессии ГА ООН. Основным итогом семинара стало подтверждение актуальности проблемы МИБ и своевременности постановки этого вопроса в международном плане. Эта первая такого рода представительная встреча экспертов, несомненно, во многом способствовала выполнению рекомендации резолюции 53/70.

На 54-й сессии ГА ООН Россией был предложен обновленный проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Проект впервые указал на угрозы МИБ применительно не только к гражданской, но и к военной сферам. 1 декабря 1999 г. резолюция (A/RES/54/49) консенсусом была принята Генассамблеей.

В этом контексте Россией был подготовлен проект «Принципов, касающихся международной информационной безопасности». Он был опубликован в документе A/55/140 в качестве вклада России в дальнейшее обсуждение темы.

Принципы представляют собой своего рода рабочий вариант кодекса поведения государств в информационном пространстве, создавая для них, по крайней мере, моральные обязательства, и закладывают основу для широких международных переговоров под эгидой ООН и других международных организаций по этой проблематике.

В них содержится необходимая понятийная база по предмету МИБ, приводятся основные определения: МИБ, угроз информационной безопасности, информационного оружия, информационной войны, международного информационного терроризма и преступности.

Пять базовых принципов МИБ определяют роль и права, обязательства и ответственность государств в информационном пространстве, намечают конкретные задачи, решение которых было бы направлено на ограничение угроз в сфере МИБ, а также прописывают роль ООН в контексте общих усилий в этой области.

Помимо российского вклада в доклад Генерального секретаря вошли также вклады Иордании, Катара и Польши.

В итоге 55-й сессии Генассамблеей 20 ноября 2000 года консенсусом был одобрен новый российский проект резолюции (A/RES/55/28), в котором отмечается, что целям ограничения угроз в сфере информбезопасности отвечало бы изучение соответствующих международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем.

Данное положение было чрезвычайно важно поскольку оно подготовило почву для следующего этапа в плане продвижения темы МИБ в ООН.

В соответствии с рекомендациями резолюции 55/28 МИД России в качестве нового российского вклада в обсуждение темы МИБ в ООН был подготовлен проект документа «Общая оценка проблем информационной безопасности. Угрозы международной информационной безопасности» (A/56/164/Add.1).

В данном документе выделены и описаны **одиннадцать** основных факторов, создающих, по мнению России, опасность основным интересам личности, общества и государства в информпространстве и представляющих, таким образом, наибольшие угрозы с точки зрения обеспечения МИБ. К таким факторам относятся, прежде всего, разработка и использование средств несанкционированного вмешательства в работу и неправомерного использования информационных ресурсов другого государства, а также нанесения ущерба им; целенаправленное информационное воздействие на критические инфраструктуры и население другого государства; действия, направленные на доминирование в информационном пространстве, поощрение терроризма и собственно ведение информационных войн.

В доклад Генсекретаря вошли также оценки Боливии, Мексики, Филиппин и Швеции (от имени государств — членов Евросоюза). Характерно, что при этом выявился определенный диссонанс и в позициях развитых государств. Они стали понимать, что даже статус союзника США не гарантирует их от электронного мониторинга со стороны своего «большого брата», причем последнее может оказываться далеко не бескорыстным. В целом ряде стран Западной Европы ведутся официальные расследования по поводу деятельности против них принадлежащей американскому правительству системы элек-

тронной разведки, прослушивания, промышленного шпионажа, сбора стратегической, в т. ч. коммерческой и частной, информации через глобальную систему «Эшелон».

В резолюции, принятой консенсусом 29 ноября 2001 г. (документ A/RES/56/19), одобрена идея создания в 2004 г. специальной Группы правительственных экспертов государств — членов ООН (ГПЭ) для проведения всестороннего исследования проблемы МИБ.

Принятая консенсусом 22 ноября 2002 г. ГА ООН резолюция по МИБ (A/RES/57/53) развивает положения предыдущих резолюций и указывает на недопустимость использования ИКТ и средств в целях оказания негативного воздействия на инфраструктуру государств. Резолюция также подтверждает просьбу к Генеральному секретарю, содержащуюся в пункте 4 резолюции 56/19, относительно создания группы правительственных экспертов ООН.

8 декабря 2003 г. Генассамблея ООН вновь консенсусом приняла резолюцию по информбезопасности (A/RES/58/32). Это решение переводит общеполитическое обсуждение проблематики МИБ в плоскость поиска практических решений и запускает механизм формирования ГПЭ, первое заседание которой прошло в июле 2004 г., второе — в марте 2005 г., третье — в июле 2005 г. Мандат Группы предусматривает проведение исследования существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, а также изучение международных концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем. Результаты работы Группы — доклад Генсекретаря ООН Генеральной Ассамблее в 2005 г., который должен задать формат и определить направления международного сотрудничества в целях реализации концепции МИБ.

В доклад Генсекретаря ООН в 2003 г. (A/58/373) вошли вклады по проблематике МИБ Боливии, Кубы, Сальвадора, Грузии, России, Сенегала и Украины. В российском документе «Вопросы, связанные с работой группы правительственных экспертов по проблеме информационной безопасности» представлено российское видение организационно-практических аспектов работы группы правительственных экспертов ООН. Группа могла бы сконцентрироваться на следующих ключевых моментах:

- согласование понятийного аппарата в сфере МИБ;
- рассмотрение факторов, влияющих на состояние МИБ с учетом наличия угроз как террористического или криминального, так и военного характера, как в военной, так и в гражданской областях;

- определение взаимоприемлемых мер предотвращения использования ИКТ и средств в террористических и других преступных целях, а также мер по ограничению применения информационного оружия, прежде всего в отношении критически важных структур государств;
- рассмотрение возможных путей международного взаимодействия правоохранительных органов по предотвращению и пресечению правонарушений в информационном пространстве, в частности, по выявлению источников информационной агрессии;
- анализ проблемы сопряжения национальных законодательств отдельных стран в части, регулирующей вопросы информбезопасности с тем, чтобы обеспечить унифицированную классификацию правонарушений в сфере информационной безопасности и ответственность, возникающую в связи с совершением действий, классифицируемых как преступные;
- оценка возможности оказания международной помощи странам, ставшим жертвами информационных атак, в целях смягчения последствий нарушения нормальной деятельности, прежде всего объектов критических инфраструктур государств.

Как представляется российской стороне, в перспективе следует стремиться к выработке многостороннего, взаимоприемлемого международно-правового документа, направленного на укрепление МИБ, в соответствии с которым государства и другие субъекты международного права должны будут нести международную ответственность за деятельность в информационном пространстве, осуществляемую ими или с территорий, находящихся под их юрисдикцией.

Основной идеей создания универсального режима МИБ могло бы стать обязательство участников не прибегать к действиям в информационном пространстве, целью которых является нанесение ущерба информационным сетям, системам, ресурсам и процессам другого государства, его инфраструктуре, подрыв политической, экономической и социальной систем, массированная психологическая обработка населения, с целью дестабилизации общества и государства.

Как уже отмечалось, в Женеве 10-12 декабря 2003 г. прошел первый этап ВВУИО, в ходе которого информбезопасность находилась в центре международного внимания.

Важную роль в этом сыграло продвижение Россией данной проблематики на подготовительных конференциях, а также на прошедшей в г.Марракеш (Марокко), с 23 сентября по 18 октября 2002 г. 16-й Полномочной конференции (ПК) Международного союза электросвязи. В ПК 2002 года приняли участие около полутора тысяч делега-

тов, представляющих 143 страны. Решением ПК был принят «Вклад МСЭ в Декларацию принципов и план действий ВВУИО» (документ PLEN/1). Одним из основных блоков в структуре вклада МСЭ в Декларацию принципов и План действий ВВУИО вошли вопросы доверия и безопасности при использовании ИКТ.

Страны также согласились внести вклад в реализацию усилий ООН, направленных на оценку состояния информбезопасности, а также рассмотрение вопроса о разработке, в долгосрочной перспективе, международной конвенции по безопасности в среде информационных сетей и сетей связи.

Формулировки по МИБ легли в основу соответствующих положений документов региональных конференций по подготовке к ВВУИО — Общеевропейской конференции (Бухарест, 7-9 ноября 2002 г.) и Азиатской конференции (Токио, 13-15 января 2003 г.), в ходе которых Россия активно продвигала проблематику МИБ.

Одним из принципов ГИО, зафиксированных в Бухарестской декларации, стал принцип укрепления доверия и безопасности при использовании ИКТ. Он подразумевает разработку «глобальной культуры кибербезопасности», которая должна обеспечиваться путем принятия превентивных мер и поддерживаться всем обществом при сохранении свободы передачи информации.

В декларации зафиксировано, что в целях содействия доверию и безопасности в использовании ИКТ органы госуправления должны способствовать осознанию обществом угроз, связанных с кибербезопасностью, и стремиться укреплять международное сотрудничество в этой сфере.

В Токийской декларации, которую приняли представители 47 стран, 22 международных, 116 неправительственных организаций и 54 частных компаний, важное место занимает вопрос обеспечения безопасности ИКТ. Признавая принцип справедливого, равного и адекватного доступа к ИКТ для всех стран, стороны особое внимание полагают уделить угрозе потенциального военного использования ИКТ. Стороны также согласились с необходимостью усилить региональное и международное сотрудничество в целях укрепления безопасности инфосферы. Впервые было зафиксировано мнение о том, что эффективное обеспечение МИБ может быть достигнуто не только технологически, но и через усилия по правовому регулированию вопроса и выработке соответствующих национальных политик.

Включение столь важных формулировок по МИБ в декларации подготовительных встреч заложило основу для последующего закрепления проблематики МИБ в повестке дня Саммита.

Как известно, итогом первого этапа Встречи в Женеве стало принятие двух документов — Декларации принципов и Плана действий. Формулировки по МИБ вошли в оба документа Встречи. В Декларации принципов (раздел «Укрепление доверия и безопасности при использовании ИКТ») указывается на то, что упрочение основы для доверия, включая информационную безопасность и безопасность сетей, является предпосылкой становления информационного общества.

В Декларации зафиксировано, что государства, принявшие ее, признавая принципы универсального и недискриминационного доступа к ИКТ для всех стран, поддерживают деятельность ООН, направленную на предотвращение возможности использования ИКТ в целях, которые несовместимы с задачами обеспечения международной стабильности и безопасности и способны оказать отрицательное воздействие на целостность государственных инфраструктур, нанося ущерб их безопасности. Они также исходят из того, что следует предотвращать использование информационных ресурсов и технологий в преступных и террористических целях.

В Плане действий отмечается, что доверие и безопасность относятся к главным опорам информационного общества. В качестве важнейших направлений действий по укреплению доверия и безопасности при использовании ИКТ в документе выделены следующие:

- содействие сотрудничеству между государствами в рамках ООН и со всеми заинтересованными сторонами в рамках соответствующих форумов в целях анализа существующих и потенциальных угроз в области ИКТ, а также решения других вопросов информационной безопасности и безопасности сетей;
- предупреждение и обнаружение органами госуправления в сотрудничестве с частным сектором проявлений киберпреступности и ненадлежащего использования ИКТ и реагирование на эти проявления путем разработки соответствующих руководящих принципов;
- изучение законодательства, которое дает возможность эффективно расследовать и подвергать преследованию ненадлежащее использование ИКТ;
- содействие эффективным мерам взаимопомощи в этой сфере, а также профилактике компьютерных инцидентов;
- обмен образцами наилучшей практики в области информационной безопасности и безопасности сетей и поощрение их использования всеми заинтересованными сторонами;
- назначение координаторов во всех заинтересованных странах для реагирования в режиме реального времени на происшествия в сфере безопасности и формирования открытой совместимой сети та-

ких координаторов для обмена информацией и технологиями реагирования на происшествия;

- поощрение активного участия заинтересованных стран в проводимой ООН деятельности по укреплению доверия и надежности при использовании ИКТ.

В декабре 2004 г. была принята очередная резолюция Генассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (см.Приложение).

Россия проводит работу в ООН и по другим аспектам проблемы информационной безопасности. Так, 20 декабря 2002 г. Генассамблея одобрила без голосования резолюцию 57/239 «Создание глобальной культуры кибербезопасности», в число соавторов которой вошла и Россия. В преамбулу включены ссылки на резолюции ГА ООН по МИБ и борьбе с преступным использованием ИКТ, что указывает на многогранность данной проблемы и наличие тесной связи между ее различными аспектами. В приложении к резолюции содержится перечень «элементов», на основе которых должна обеспечиваться безопасность сетей — от этики и демократии до ответственности и управления обеспечением безопасности.

17-18 июня 2002 г. в Нью-Йорке состоялось двухдневное заседание 56-й сессии Генассамблеи ООН, посвященное использованию ИКТ в целях развития, в котором приняла участие и российская делегация. В ходе состоявшихся дискуссий сформировался общий консенсус в отношении потенциала ИКТ в том, что касается поощрения устойчивого роста, борьбы с нищетой, укрепления демократического правления и ликвидации различных видов неравенства в процессе преодоления «цифрового разрыва». ИКТ были оценены участниками сессии как стратегический инструмент достижения целей в области развития, а Генассамблея — как наиболее универсальный и представительный орган системы ООН, являющийся форумом для разработки значимых, ориентированных на конкретные действия по преодолению «цифрового разрыва» и способствующий тем самым реализации целей, зафиксированных в Декларации тысячелетия.

Результирующая политической борьбы по проблеме МИБ на сегодняшний день заключается в том, что международное сообщество вполне понимает ее существо и актуальность, признает необходимость воспользоваться моментом, созданным российской инициативой, для создания совместными усилиями международных организационно-правовых условий или, своего рода, кодекса поведения государств в информационном пространстве для цивилизованного развития технологического прогресса в мире.

5.3.3.Усилия России по борьбе с информационным терроризмом

Важный блок проблем, непосредственно относящийся к ИКТ и инфосфере и курируемый ООН, включает в себя нормотворческую деятельность, актуальность которой резко возросла в контексте усиления борьбы мирового сообщества с международным терроризмом и преступностью.

4 декабря 2000 г. и 19 декабря 2001 г. Генассамблея одобрила продвигавшиеся США и другими развитыми странами резолюции 55/63 и 56/121 под общим названием «Борьба с преступным использованием информационных технологий», направленные на создание правовой основы для этой цели. Россия поддержала эти документы. Она также проголосовала за резолюцию 1373 (2001), принятую Советом Безопасности ООН в связи с крупномасштабным терактом против США 11 сентября 2001 г. В этом документе, наряду с другими мерами по борьбе с терроризмом, содержится призыв к государствам-членам к организации и ускорению обмена информацией, в том числе об использовании террористами ИКТ. В соответствии с резолюцией 57/171 от 18 декабря 2002 г. один из семинаров 11-го Конгресса ООН по предупреждению преступности и уголовному правосудию посвящен мерам по борьбе против преступлений, связанных с использованием высоких технологий и компьютеров.

Незаконные вооруженные формирования и организации террористической, экстремистской, радикальной политической, радикальной религиозной направленности все шире используют ИКТ для своих преступных целей:

- создают собственный, в т.ч.закрытый сегмент информационного пространства, стремятся к захвату или контролю (а также к разрушению и замещению на собственный) сегментов национального и/или глобального информационного пространства;
- создают в рамках своих или родственных структур силы, в функции и задачи которых входит ведение информационного противоборства;
- используют научно-технический потенциал, в т.ч. союзников, а также поддерживающих их стран для разработки и испытаний образцов и систем информационного оружия, средств его доставки и маскировки, принципов применения, а также приобретают при необходимости (чаще всего тайно) данные средства у союзников или третьей стороны;

Наряду с активным участием России в подготовке и реализации важных решений по борьбе с терроризмом в рамках ООН, «восьмер-

ки», ЕС, ОБСЕ, СЕ и др., на заседании Совета Россия — НАТО 9 декабря 2004 г. был утвержден План действий по борьбе с терроризмом, в котором представляется оправданным выделить следующие аспекты.

1. Совет Россия — НАТО категорически отвергает терроризм во всех его проявлениях. Террористические акции представляют прямой вызов нашей общей безопасности, нашим общим демократическим ценностям, а также основным правам и свободам человека. Никакие причины не могут оправдать подобные акции, и призываем к единству действий международного сообщества в борьбе с этой коварной угрозой. Мы сделаем все, что в наших силах, для борьбы со всеми формами терроризма, действуя в соответствии с Уставом ООН, международным правом прав человека и международным гуманитарным правом, а также другими существующими обязательствами. Мы едины в поддержке резолюций 1368, 1373, 1540, 1566 и всех других соответствующих резолюций Совета Безопасности ООН и не пожалеем усилий в рамках СРН и других соответствующих форумов для защиты наших граждан, для достижения нашей общей цели — привлечь к ответственности исполнителей, организаторов, подстрекателей и спонсоров террористических акций, перекрыть каналы финансирования террористической деятельности и победить зло терроризма, в том числе посредством ратификации и эффективного выполнения международных конвенций, относящихся к терроризму, в т.ч. двенадцати антитеррористических конвенций и протоколов ООН.

2. Совет может и должен внести еще более непосредственный и существенный вклад в эту глобальную борьбу, если необходимо, во взаимодействии с другими партнерами. Сотрудничество в СРН в области борьбы с угрозой терроризма должно быть прагматичным и целенаправленным, дополняющим и подкрепляющим усилия, предпринимаемые в рамках других форумов. Как согласовано главами государств и правительств СРН в Римской декларации от 28 мая 2002 г. наше сотрудничество должно быть «многоплановым», как и сама угроза терроризма. Наша цель — повысить наши возможности действовать, индивидуально и совместно, в трех областях, имеющих критически важное значение:

- предотвращение терроризма;
- борьба с террористической деятельностью;
- устранение последствий террористических акций.

В речи на заключительном пленарном заседании Международной встречи на высшем уровне по вопросам демократии, терроризма и безопасности «Глобальная стратегия борьбы с терроризмом» (Мадрид,

10 марта 2005 г.) К.Аннан подчеркнул, что «*терроризм — это угроза всем государствам и всем народам, которая может проявиться в любой момент и в любом месте*». Одновременно он предложил пять элементов действий (по-английски «пять D»). Это:

- во-первых, *разубедить* недовольные группы использовать терроризм в качестве тактического средства для достижения своих целей;
- во-вторых, *лишить* террористов средств для совершения нападений;
- в-третьих, *удержать* государства от оказания поддержки террористам;
- в-четвертых, *создать государственный потенциал* для предотвращения терроризма;
- и в-пятых, *защищать* права человека в борьбе с терроризмом.

К.Аннан особо отметил, что ООН и ее специализированные учреждения играли центральную роль в выработке путем переговоров и в принятии 12 международных договоров о борьбе с терроризмом. Теперь пришло время завершить работу над всеобъемлющей конвенцией, ставящей вне закона терроризм во всех его формах.

Теракты 2005 г. в Лондоне, Египте, Турции и других странах императивно диктуют необходимость ускорения принятия указанной конвенции, проект которой содержит и информационную составляющую терроризма, т.к. террористы используют и информационное оружие

Так, в сети на протяжении нескольких лет существовал сайт чеченских сепаратистов kavkaz.org, открыто выступавший не только против проведения контртеррористической операции в Чеченской Республике, но и призывающий бороться против федеральных властей[20].

Kavkaz.org неоднократно пытались ломать. В марте 2002 г. группа хакеров, скрывающаяся под псевдонимом «Сибирская сетевая бригада» смогла частично ликвидировать сайт. При попытке открыть электронную страницу на экране появлялись сообщения антитеррористической направленности. На следующий день после теракта в ДК на Дубровке пропагандистский сайт был ликвидирован группой российских программистов, но вскоре он опять начал функционировать.

Исходя из мировой практики, создается впечатление, что действия программистов — возможно, единственный адекватный ответ на акции сетевых провокаторов. Законодательные меры оказываются не-

[20] http://www.cnews.ru/newcom/index.shtml?2004/10/29/167388

эффективными. В сентябре 2003 г., суд Вильнюса признал незаконными действия литовского Департамента госбезопасности, который в июне 2003 г. закрыл сайт «Кавказ-Центр». Тогда создателей интернет-ресурса обвинили в пропаганде терроризма, национальной и религиозной розни. Были проведены обыски в офисе фирмы, которая размещала электронную страницу на своем сервере. Закрыть «Кавказ-Центр» требовали от Литвы и Российские власти. Однако уже в конце сентября 2003 г. суд Вильнюса вынес решение в пользу создателей сайта.

Другой, не менее интересный пример: в апреле 2003 г. руководство Эстонии ответило отказом на требование России запретить одной из коммерческих фирм этой прибалтийской страны сотрудничать с чеченскими террористами. Как сообщала телекомпания НТВ, данная структура предоставляла чеченским экстремистам услуги по размещению Интернет-сайта боевиков. По словам эстонского премьер-министра, «сайт находится не на сервере правительства Эстонии, поэтому кабинет в его деятельность вмешиваться не станет, несмотря на то, что Россия требует его закрыть».

13 сентября 2004 г. после ряда террористических актов МИД России вновь потребовал прекращения работы сайта чеченских боевиков «Кавказ-Центр». Для этого в МИД был вызван посол Литвы в России Р. Шидлаускас. Как говорилось в сообщении ведомства, вопрос был поставлен перед ним «в жесткой форме», и 19 сентября власти Литвы временно заблокировали чеченский информационный сайт. Однако вскоре он опять был открыт, но уже в Финляндии, а после очередной ноты протеста российского правительства, вновь был закрыт.

Все чаще террористы берут на себя ответственность через Интернет или вывешивают на своих сайтах фотографии жертв, взрывов и даже видеоролики отснятых терактов. Нередко посредством своих ресурсов боевики отчитываются о проделанной работе или обращаются с посланиями к определенной категории граждан. С помощью Интернета террористы запугивают общественность, угрожая новыми террористическими атаками.

В настоящее время во Всемирной сети существует уже несколько сотен экстремистски настроенных информационных ресурсов. Если в 1998 г. примерно половина из 30 организаций, которых США причисляли к террористическим, обладали своими электронными страницами, то ныне в сети представлены абсолютно все известные своими радикальными взглядами группы. Причем материалы они переводят не менее чем на 40 различных языков.

Все более-менее серьезные представители экстремистских организаций располагают не только веб-сайтами, но и форумами, и досками объявлений, где могут пообщаться их сторонники. Террористы из группировки «Хамас», например, создали несколько сайтов, ориентированных на детей. А их «коллеги» из «Хезболлах» пошли еще дальше: ее поклонники могут скачать с сайта группировки видеоигру, сюжет которой — война с израильтянами в Ливане. В сети можно разыскать тексты выступлений Бен Ладена, книги по идеологии джихада, информацию о проведенных терактах и ознакомиться с лучшими образцами джихадской поэзии.

Как сообщила газета The Washinfton Times за 29 июня 2004 г., наиболее активным пользователем всемирной паутины среди террористов является Абу Мусаб аль-Заркави, возглавляющий ячейку «Аль-Каиды» в Ираке. Он использует сеть Интернет для вербовки сторонников и сбора средств на проведения террористических актов, направленных против сил коалиции и нового иракского правительства.

Американцы пытаются оперативно закрывать сайты, на которых «засветился» известный террорист. Однако Аль-Заркави каждый раз находит новый способ публиковать во всемирной сети факты своих деяний. Связь через всемирную компьютерную сеть идеально подходит для террористов. По некоторым данным, подготовка к терактам 11 сентября велась именно с помощью обмена зашифрованными посланиями по электронной почте. «Аль-Каида» поддерживает сейчас в Сети порядка 50 различных сайтов.

Администрации многих стран в меру сил пытаются бороться с проявлением кибертеррора. В конце 2003 г. США впервые внесли в свой список иностранных террористических организаций несколько Интернет-сайтов. Согласно американскому законодательству, эти ресурсы теперь вне закона и запрещена любая материальная поддержка этих сайтов, их сотрудникам запрещен въезд на территорию США, а американские банки должны заморозить их счета. Однако, как сообщило агентство Reuters, даже сам Госдепартамент пока не понимает, каким образом это будет сделано.

Единственный метод, которым можно, с точки зрения официальных лиц, остановить появление террористов-самоучек, — это цензура. Нечто подобное после 11 сентября 2001 г. практиковали США. Тогда из общего доступа были удалены многие ресурсы, представляющие хоть какую-то ценность для потенциальных террористов. Цензура введена и на территории Китая, где, помимо всего прочего, ограничен доступ к зарубежным СМИ.

Совсем не случайно Ю.М.Лужков опубликовал 16 мая 2004 г. в газете «Известия» статью «О темной стороне Интернета». Основной смысл статьи сводился к тому, что необходим специальный закон об Интернете, каким-либо образом регламентирующий распространение информации.

Подобные меры, принимаемые в ряде стран, востребованы, хотя и не всегда являются популярными. Возможно, что с течением времени образуются учреждения, предсказываемые М.Кастельсом, так называемые «on-line полицейские патрули». Первые прототипы подобных организаций появились в августе 2004 г. во Вьетнаме, там было сформировано специальное полицейское подразделение, в задачи которого входит расследование онлайн-преступлений и слежка за распространением запрещенных публикаций в киберпространстве. Структуры, следящие за содержанием Интернета, безусловно, востребованы уже сегодня.

Результаты последних исследований свидетельствуют, что идея введения паспортов с биометрической идентификацией не столь совершенна, как об этом говорят ее сторонники. Современные технологии позволяют преступникам без особого труда «клонировать» любые документы[21].

Издание Australian IT цитирует ведущего специалиста лабораторий RSA Барта Калиски (Burt Kaliski), который отмечает, что, несмотря на растущее распространение радиочастотных идентификационных устройств, данная технология в долгосрочной перспективе «не настолько надежна, как следовало бы». «Это особенно важно, поскольку паспорта в США рассматриваются как следующая огромная область для внедрения RFID, — указал он. — Результаты исследований показывают, что удаленное сканирование широко распространенных ныне RFID-ярлыков, позволяющее создавать их идентичные копии, возможно уже сегодня. Становится возможным «клонировать» оригиналы».

RSA предсказывает рост спроса[22] на системы пользовательской идентификации на базе радиочастотных устройств как для обеспечения защиты компьютерных сетей, так и для контроля доступа в помещения.

Такие системы существуют уже сегодня в виде электронных пропусков, передающих информацию в радиочастотном диапазоне. Если злоумышленник может, пройдя мимо человека, просканировать пропуск,

[21] http://www.cnews.ru/newtop/index.shtml?2005/03/01/175333

[22] http://www.cnews.ru/newtop/index.shtml?2005/01/14/172741

лежащий у того в кармане или в сумочке, а затем изготовить его электронную копию, для системы охраны он станет идентичной копией своей жертвы. RFID-системы потенциально чрезвычайно уязвимы, и остается только надеяться, что эта их уязвимость не проявится на практике.

Причем сама по себе биометрия безопасность не повышает, подчеркивает Барт Калиски, поскольку вопрос — не в уязвимости биометрии как таковой, а в уязвимости чипов, используемых для хранения биометрической информации.

В настоящее время рассматривается возможность введения так называемой «комбинированной биометрии», при которой у идентифицируемого человека запрашивается лишь информация о том, кем именно он является, — но сам его чип биометрической информации не содержит. Его отпечатки пальцев или рисунок радужки сравниваются с образцами, полученными системой из имеющихся баз данных. В этом случае сканирование RFID-чипа позволит лишь установить, кем именно является данный человек, однако не позволит злоумышленнику в полной мере «подменить» его. Если же сканирование RFID-устройства позволит получить доступ еще и к биометрическому «паспорту» человека, тогда подмена становится делом вполне возможным.

Учитывая вышеизложенное, Федеральное агентство по техническому регулированию и метрологии РФ направило в международный подкомитет по стандартизации в области биометрии при ИСО (The International Organisation for Standardisation) официальное предложение по изменению международного стандарта в области биометрии.

Суть предлагаемой поправки заключается во включении трехмерного цифрового изображения лица, наряду с обычной двухмерной фотографией, в формат данных, предназначаемый для хранения, обмена и использования при автоматическом распознавании личности.

Трехмерная фотография — новейшая биометрическая технология, которая появилась около 5 лет назад и была изобретена отечественными разработчиками. Занимая всего 5 килобайт, трехмерное фото может быть записано в биометрический паспорт и позволяет увеличить точность идентификации личности при допуске в помещения или при пересечении государственных границ и повысить надежность автоматической сверки документов.

На заседании Международного подкомитета по стандартизации в области биометрии (ISO/IEC JTC1/SC37 Biomerics) предложение было поддержано всеми странами-участницами. Более того, Международный подкомитет в целях ускорения работы над стандартом, не дожи-

даясь официальных результатов голосования, уже сформировал редакторскую группу, в которую вошли 12 соредакторов из разных стран.

Эта первая инициатива России по разработке международных стандартов не только в области биометрии, но и вообще в области высоких технологий. Наши эксперты подготовили это предложение, и в содружестве с коллегами по 37 подкомитету из США и Австралии была разработана техническая спецификация, которая ляжет в основу проекта данного стандарта. В процессе обсуждения на заседании рабочей группы предложение было одобрено экспертами всех стран — членов подкомитета.

Уровень распознавания трехмерной фотографии составляет более 90%, тогда как у двухмерного изображения этот показатель редко превышает 50%, отмечают эксперты НИИ «Восход», который утвержден российским правительством в качестве главного координатора по созданию новой системы биометрических паспортов.

Ранее, в феврале 2005 г., по инициативе компании A4vision, поддержанной Oracle, Motorola, Unysys, Logitech и др., аналогичная поправка к американскому национальному стандарту была одобрена в США. Компания A4vision, основанная нашими соотечественниками, первая разработала технологию трехмерного распознавания лиц и, выйдя на рынок США, инициировала процедуру изменения американского стандарта.

Первая версия нового международного стандарта должна быть согласована и опубликована рабочей группой до 15 ноября 2005 г. и утверждена на следующем заседании международного подкомитета, который состоится в январе 2006 г. в Японии.

Таким образом, формирование ГИО привело к появлению новых рисков и угроз национальной безопасности государств и международной безопасности в информационной сфере. К ним, в частности, относятся кибертерроризм, киберпреступность, а также негативное информационно-психологическое воздействие на человека с использованием ИКТ.

Россия активно участвует в многостороннем и двустороннем сотрудничестве по борьбе с киберпреступностью, выступает за разработку международной стратегии комплексного противодействия киберугрозе и создание единых международно-правовых механизмов с целью унификации национальных уголовных законодательств.

Одним из таких механизмов стала вступившая в силу 1 июля 2004 г. Конвенция о киберпреступности. Однако ограниченный круг ее участников (ни одна из стран «восьмерки» ее не ратифицировала) не позволяет придать ей универсальный характер, т.к. общее число

стран, ратифицировавших Конвенцию (на август 2005 г.) – всего 11. Россия не участвовала в разработке данной Конвенции, вследствие чего некоторые ее положения, например невозможность принятия оговорок по целому ряду статей, являются препятствием для ее подписания. Это касается, в частности, статьи 32, которая при определенных условиях позволяет правоохранительным органам одного государства-участника Конвенции проводить оперативно-розыскную деятельность на территории другого государства-участника Конвенции, что представляет собой потенциальную угрозу национальной безопасности.

В рамках «Группы восьми» эффективно функционирует подгруппа по борьбе с преступлениями в сфере высоких технологий Римской/Лионской группы. В 1998 году создана Сеть Национальных Контактных Пунктов Министерств внутренних дел, в работе которой принимает участие 40 государств в режиме реального времени.

В условиях активизации деятельности международных террористических и экстремистских организаций стала реальной угроза совершения нападений на критически важные объекты — информсистемы управления вредных и опасных производств, энергетики, транспорта, связи и госучреждений. Помимо кибератак также возможны попытки злоумышленников добиться от органов госвласти выполнения политических требований путем угрозы распространения сведений, составляющих гостайну. В мае 2005 г. в США состоялись первые международные учения в рамках «восьмерки» по отражению кибератак и защиты критически важных объектов от террористов.

Своим отдельным Решением СМИД ОБСЕ в декабре 2004 года призвал государства-участники обмениваться информацией об использовании Интернета в террористических целях и определять возможные стратегии борьбы.

Расширяется двустороннее сотрудничество России в сфере противодействия киберугрозе в рамках Рабочих групп по борьбе с терроризмом с США, Великобританией, Индией, Китаем, Пакистаном и т.д. Вопросы противодействия киберпреступности органично вошли в их общие программы действий.

Анализ складывающейся обстановки в столь важном вопросе показывает, что эффективное противодействие таким угрозам невозможно силами отдельного государства. Одиннадцатый Конгресс ООН по предупреждению преступности и уголовного правосудия (Бангкок, 18 – 25 апреля 2005г.) стал важной вехой в решении данной задачи.

Резюмируя, можно со всей ответственностью заявить, что единственным соразмерным угрозе решением проблемы остается создание международного механизма ограничения гонки информационного оружия и предотвращения информационных войн. Альтернатива иррациональна — мировой информационный апокалипсис.

И последнее. В **Концепции внешней политики России** подчеркнуто, что осуществление крупного прорыва на ряде ключевых направлений научно-технического прогресса, ведущего к созданию единого общемирового информационного пространства, придают взаимозависимости государств глобальный характер. В силу этого совершенно очевидно, что для построения более стабильного и кризисоустойчивого многополюсного мира, дипломатия должна, опираясь на современные информационные технологии, находить оптимальные решения самых сложных дилемм российской внешней политики.

И несомненно, что одна из ключевых из них — это международная информационная безопасность.

ВМЕСТО ЗАКЛЮЧЕНИЯ

Для успеха не надо быть намного умнее других,
надо просто быть на день быстрее большинства.

СЦИЛЛАД

Императив информационной глобализации для России: инновационная конкурентоспособность

Осмысливая изложенное в монографии, представляется оправданным сделать следующие умозаключения.

1. Глобализация, выражающаяся в лавинообразном увеличении потоков информации, технологий, капитала, товаров, услуг и людей во всем мире, стала всеохватывающей мегатенденцией.

Информационная революция открыла принципиально новую главу в развитии цивилизации, стала локомотивом и нервом процессов глобализации, придавая ей все более необратимый характер.

2. Феномен информационной глобализации оказывает преобразующее воздействие на все сферы жизнедеятельности — экономику, политику, безопасность, социальную сферу, науку, культуру, образование и досуг. Взаимодействие различных стран и регионов в процессе освоения и применения результатов ИКТ становится одной из самых динамичных и многообещающих сфер международного сотрудниче-

ства. Данная проблематика, в т.ч. и с учетом негативной составляющей, в последнее время позиционируется как ведущая в деятельности ООН, ЮНЕСКО, ВТО, «восьмерки», МСЭ, ОЭСР, Евросоюза, АТЭС и других важных международных и региональных организаций и структур. **Одновременно ИКТ оказывает влияние на саму деятельность международных организаций, способствуя не только повышению их эффективности, но и ускорению процессов их реформирования (реинжиниринга).**

3. Самые большие **выгоды от глобализации получают те страны и группы, которые быстрее переходят на инновационный путь развития**. Спрос на ИКТ неуклонно растет, их возможности стремительно расширяются. Доля ИКТ в структуре ВВП ведущих стран увеличивается и достигает от 5 до 20%, а общемировые темпы роста на уровне 8-9% в год значительно превышают темпы развития отраслей «индустриальной» экономики. ИКТ заняли одно из ведущих мест в структуре международной торговли, их доля в настоящее время превышает объемы международной торговли вооружением и военной техникой.

Рост отрасли ИКТ в меньшей степени зависит от традиционных факторов производства: размеров инфраструктуры и объемов имеющихся природных ресурсов. **Ключевым фактором успешного развития ИКТ является качество человеческого капитала и его интеллектуальный потенциал**. Это создает широкие возможности для успешной интеграции в мировую экономику многих развивающихся стран.

Назревающая «суперреволюция» в высоких технологиях путем слияния нано-, био-, ИКТ и материальных технологий открывает не только перед представителями «первого мира», но и перед «азиатскими тиграми», Бразилией, Индией, Китаем и рядом других стран, ведущих фундаментальные исследования в этих сферах, возможность стать лидерами в ряде критически важных, «прорывных» направлений (от создания искусственного интеллекта до кибервоинов), способных существенно изменить глобальное развитие.

4. **Национальное государство, оставаясь важнейшим конструктивным элементом мирового порядка, в условиях информационной глобализации и неизбежности организации функционирования электронного правительства, испытывает все большие нагрузки в повышении эффективности управления, борьбе с коррупцией, адекватном обеспечении транспарентности, осуществлении «обратной связи», электронной демократии и т.д.** Одновременно ТНК в области ИКТ и крупные фирмы-провайдеры становятся все менее подконтрольны какому-либо из государств. При этом исповедуемый ими курс на телетруд и крупномасштабный аутсорсинг лишь усиливает антиглобали-

стское движение, т.к. в первую очередь ставит под удар средний класс развитых стран.

Массовое возникновение виртуальных сообществ со своими собственными интересами (к примеру, в России с 2003 г. движение «флэшмоб»[1] — неожиданное появление и исчезновение в общественном месте сотен объединенных общим девизом участников, что приводит в замешательство не только публику, но и правоохранительные органы) весьма затрудняет работу «неперестроившихся» органов госвласти. Кроме этого, **в Интернете уже зафиксированы попытки создания различных транснациональных движений, которые способны влиять не только на государство, но и стать заметной силой в международных отношениях.**

5. ИКТ, дающие возможность для непрерывного обмена информацией, в т.ч. зашифрованной, способствуют все большей децентрализации террористической угрозы, исходящей от многообразных группировок и отдельных террористов, не нуждающихся в штабах для планирования и проведения операций. Виртуализуются и учебные материалы по их спецподготовке, выбору целей, оружейному ноу-хау, сбору средств, операциям прикрытия и т.д. **Серьезная заинтересованность террористов в приобретении не только химического, биологического, ядерного оружия, но и информационного оружия при их комбинации драматически усиливает угрозы и риски, повышает вероятность крупных терактов с применением ОМП.**

Принимаемые международным сообществом меры по борьбе с международным терроризмом пока не столь эффективны. Одна из причин — в его оценках, т.к. даже после ужасной трагедии 11 сентября 2001 г. в США в некоторых странах все еще не был изжит «двойной стандарт». Страшные теракты 2005 г. в Лондоне, Египте, Турции и ряде других стран должны, наконец, положить конец этой порочной практике.

В рассекреченном в 2005 г. документе, подготовленном по заказу ЦРУ под названием «Контуры мирового будущего: доклад по проекту — 2020» Национального разведывательного совета США, намечены пути и проблемы развития цивилизации и предлагаются несколько возможных вариантов будущего[2].

1. **«Давосский мир»** иллюстрирует, каким образом уверенный экономический рост, во главе которого встанут Китай и Индия, способен в ближайшие 15 лет изменить направление процессов глобализа-

[1] См. http://www.fmob.ru

[2] http://www.from-ua.com/politics/42493dd1c215d/

ции, придав им менее западный облик и одновременно преобразуя поле политической игры.

2. **Pax Americana** дает представление о том, каким образом США могут сохранить свою доминирующую роль при радикальных изменениях мирового политического пейзажа и повлиять на формирование нового всеобъемлющего мирового порядка.

3. **New Caliphate** представляет пример всемирного движения, которое подпитывается радикальной религиозной политикой и бросает вызов западным нормам и ценностям, становясь фундаментом новой системы.

4. **«Кольцо страха»** служит примером того, что обеспокоенность распространением ОМП может привести к крупномасштабным превентивным интервенциям, направленным на предотвращение смертоносной угрозы, и что **результатом этих интервенций может стать создание оруэлловского мира**.

Особое внимание составители доклада уделяют потреблению энергии, которое к 2020 г. вырастет примерно на 50% (в 1980—2000 гг. рост составил 34%), причем нефть будет занимать все большую долю.

В этом контексте авторы анализируют **роль России**, которая, по их мнению, способна усилить свою международную роль благодаря статусу крупнейшего экспортера нефти и газа. При этом авторы отмечают, что Россия стоит перед серьезным демографическим кризисом, вызванным низкой рождаемостью, упадком здравоохранения и потенциально катастрофической ситуацией с распространением СПИДа. На юге она граничит с нестабильным кавказско-среднеазиатским регионом, откуда весьма вероятно дальнейшее проникновение в Россию мусульманского экстремизма, терроризма и локальных конфликтов. Заключая, **авторы доклада прогнозируют, что, хотя эти социально-политические факторы ограничивают возможное значение России в глобальной политике, Москва, скорее всего, станет важным партнером и для существующих держав — США и Европы, и для новых держав в лице Китая и Индии.** Попытку оппонировать авторам доклада во второй части книги[3] сделал А.Шубин в статье «Россия-2020: будущее страны в условиях глобальных перемен», где автор предлагает три сценария будущего для нашей страны, суть которых сводится к следующему:

1. **«Конец истории»** — глобализация показала способность справиться с важнейшими вызовами. Россия полностью интегрировалась

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

в систему глобализма в качестве периферии, а ее элита — в мировую элиту на подчиненных ролях. Сетевые структуры полностью подчинены глобальной информационной олигархии, контролирующей институты мирового правительства.

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

3. **«Третья волна во втором эшелоне»** — в России сознательно создается, в частности, социально-креативный постиндустриальный уклад, полномочное самоуправление, защита и поддержка гражданского общества и корневых информационных структур. В интересах этих преобразований возможно использование «неосоветского возрождения снизу». Использование опыта стран «первого эшелона» в преодолении «третьей волны» облегчит этот переход России.

Оставив на совести авторов доклада некоторые оценки будущего России, равно как и отвергая первые два сценария А.Шубина (поблагодарив его за футурологически интересные версии глобальных угроз), еще раз (подробно — в главе 4) отметим следующее.

1. Российский рынок ИКТ демонстрирует опережающие по отношению к экономике страны в целом и одни из самых высоких в мире темпы роста на уровне 20 % в год (хотя во многом это обусловлено низким первоначальным уровнем их использования и высоким спросом на них).

Несмотря на значительные темпы роста российского рынка ИКТ, отечественное производство конкурентоспособной продукции в этой сфере только формируется и по уровню развития отстает не только от западных стран, но и от некоторых стран Восточной Европы и Азии.

Из-за отсутствия собственного производства компьютерного оборудования и базового программного обеспечения (ПО), соответствующего мировому уровню, большая часть российских предприятий в сфере ИКТ не создает продукции с высокой добавленной стоимостью, а поставляет на рынок продукцию зарубежных производителей.

2. С учетом того, что ключевым фактором успеха на мировом рынке ИКТ является квалификация специалистов, их интеллектуально-творческий потенциал, для успешной конкуренции в этой сфере в России имеется целый ряд серьезных предпосылок. Разработка новой продукции в сфере ИКТ, особенно ПО, в целом соответствует

профилю высшего образования, т.к. в России создана эффективная система подготовки инженеров и специалистов в сфере прикладной математики, вычислительной техники и программирования, конкурентоспособных на мировом рынке труда. Студенты российских вузов неоднократно выигрывали и становились призерами всемирных олимпиад по программированию.

Несмотря на традиционные проблемы в изучении иностранных языков и классических управленческих дисциплин, специалисты в сфере ИКТ пользуются высоким спросом за рубежом.

3. Некоторые предприятия имеют опыт успешного выполнения масштабных проектов разработки ПО для крупных зарубежных корпораций, однако объемы этих работ невелики по сравнению со странами-конкурентами, а производство сконцентрировано в Москве и Санкт-Петербурге. **В других регионах страны отсутствует современная инфраструктура поддержки интеллектуального, ориентированного на экспорт производства в сфере ИКТ, отвечающая международным стандартам**. Это приводит к дальнейшей «утечке мозгов», а русскоговорящие специалисты в сфере ИКТ из ближнего зарубежья, которые могли бы стать ресурсом развития отечественной отрасли, также предпочитают развитые страны из-за ограничений существующего миграционного законодательства. Развитие отечественной отрасли ограничивает также недоступность финансовых ресурсов и отсутствие механизмов венчурного финансирования перспективных проектов.

4. **Развитие ИКТ сдерживается и существующими административными барьерами.** Действующий порядок таможенного оформления экспорта продукции в сфере ИКТ приводит к задержкам и росту расходов компаний, стимулируя увод экспортных операций за рубеж. Применяемые органами госвласти механизмы защиты информации усложнены необходимостью получения для каждой сделки сертификатов и лицензий ФАПРИД.

Специфика экспорта ПО и другой продукции и услуг в сфере ИКТ не описана в законодательстве, что усложняет подтверждение факта экспорта ПО и ИКТуслуг по каждой сделке для возврата налога на добавленную стоимость и приводит к потере доходов бюджета, т.к экспорт осуществляется через филиалы и дочерние компании. Использование подобных схем затрудняет возможность получения кредитов и венчурного финансирования, а также осложняет поиск партнеров в России и за рубежом.

Налогообложение расходов по оплате труда в себестоимости производства компаний отрасли составляет от 60 до 70 %. **Применение**

действующих ставок единого социального налога снижает конкурентоспособность компаний на мировом рынке. На практике это приводит к переводу центров капитализации российских компаний в страны с более благоприятным налоговым климатом

Объем иностранных инвестиций в отрасль остается крайне низким из-за отсутствия эффективных механизмов защиты прав интеллектуальной собственности и специальных мер налогового стимулирования инвестиционной активности в этой сфере.

5. Мировой опыт показывает, что превращение отрасли ИКТ в одну их движущих сил модернизации страны возможно только в случае обеспечения господдержки ее развития.

Достижение показателей развития отрасли ИКТ к 2010 г., сопоставимых с показателями ведущих стран, требует ускоренного развития отрасли на уровне 40-45 % в год.

Сохранение существующей ситуации в ближайшее время приведет к невозможности эффективного использования имеющегося интеллектуально-творческого потенциала страны, продолжению «утечки мозгов», увеличению технологического отставания России, сохранению высокой зависимости от «ископаемой» экономики и импорта высокотехнологичной продукции.

Если не принять меры по обеспечению господдержки отрасли ИКТ, можно спрогнозировать:

- С 2007 г., по мере насыщения российского рынка зарубежной продукцией, замедление темпов роста его основных сегментов до уровня 10–12 % в год.
- Сохранение позиции нетто-импортера ИКТ и услуг, лишение экспортных возможностей, предоставляемых на период до 2010 г. ростом рынка международного аутсорсинга в сфере ИКТ, до 140 млрд долл. США.
- Консервация отставания России по уровню использования ИКТ от стран 2 группы по классификации ОЭСР.
- Сохранение обеспечивающей роли отрасли ИКТ в национальной экономике.
- Снижение конкурентоспособности и как следствие экспортного потенциала базовых отраслей экономики и выход стратегических инвесторов из российских компаний.
- Постепенное **перетекание национальных интеллектуальных ресурсов в развитые страны** и их концентрации в корпорациях «инфономики».

Анализ мирового опыта показывает, что господдержка развития национального производства в сфере ИКТ может быть направлена на решение следующих приоритетных задач:

- развитие производства в сфере ИКТ, ориентированного на удовлетворение внутреннего спроса, включая импортозамещение;
- развитие научных разработок, производства ПО и предоставления услуг, ориентированноых, прежде всего, на мировой рынок.

Опыт Латинской Америки, в частности Бразилии, показывает, что политика протекционизма требует от государства значительных бюджетных затрат на стимулирование развития ИКТ на протяжении продолжительного периода, так как в отсутствие конкуренции со стороны иностранных производителей национальные компании не имеют стимулов к совершенствованию продукции и созданию новых товаров и услуг.

Мировой опыт также показывает, что ключевым направлением обеспечения господдержки в рамках развития ИКТ является создание специализированных технологических парков. Их создание в России позволит:

- обеспечить территориальную концентрацию финансовых и интеллектуальных ресурсов для производства ИКТ и услуг;
- снизить издержки на использование инфраструктуры;
- получить доступ к передовым знаниям и опыту;
- обеспечить эффективное привлечение кадров и занятость достаточно большого количества специалистов;
- применять методы финансового (налогового и таможенного) стимулирования;
- решить задачу привлечения ведущих компаний для открытия исследовательских центров, центров перспективных разработок и производств;
- использовать финансовые, промышленные и управленческие ресурсы международных компаний;
- создать в стране новые высокооплачиваемые рабочие места и развивать инфраструктуру;
- способствовать приобретению российскими специалистами передового опыта управления проектами в сфере ИКТ.

Существующим примером взаимовыгодного сотрудничества является открытие в России центров разработки и исследований таких лидеров ИКТ, как «Интел», «Моторола», «Боинг», «Сан Майкросистемс» и др.

Программа создания в стране пяти технопарков (см. приложение), наряду с Национальной концепцией информационного развития и другими важными мероприятиями, лежит в основе **среднесрочной программы социально-экономического развития экономики России на 2005-2007 годы**. Последняя содержала три сценария.

Первый — инерционный, рассчитывающий на благополучную внешнеэкономическую конъюнктуру и на то, что сырьевой экспорт обеспечит экономический рост.

Второй — экспортно-инвестиционный, создающий условия для больших инвестиций и развития отдельных секторов экономики.

Третий — инновационный, который, как заявил премьер-министр России М. Фрадков, выступая на церемонии награждения лауреатов премий правительства в области науки и техники**, и был взят за основу**.

Новые явления в жизни мирового сообщества, связанные с интенсивным проникновением ИКТ во все сферы деятельности человека, общества и государства, делают еще более очевидной **значимость информационно-коммуникационной составляющей внешней политики России**.

Наряду с обеспечением дипломатическими средствами благоприятных внешних условий для внутреннего развития страны, в иерархии приоритетов **на одно из самых важных направлений выдвигается задача международно-правового регулирования эффективного вхождения России в глобальное информационное общество с обеспечением при этом всех аспектов национальной безопасности**. В условиях все более активной разработки и применения, в т.ч. террористами, информационного оружия критическую важность приобретает реализация концепции международной информационной безопасности. В противном случае человеческая цивилизация обречена на апокалипсис по первым двум сценариям А.Шубина.

Резюмируя, можно со всей определенностью констатировать, что Россия обречена на инновационное развитие. Альтернативные варианты в условиях информационной глобализации иррациональны. Категорический императив — сделать это нужно как можно быстрее и умнее.

ГЛОССАРИЙ

Глоссарий содержит лишь незначительную часть терминологии, которая, по мнению автора, поможет полнее понять изложенный в монографии материал. При составлении глоссария были использованы «Толковый словарь современной информационно-правовой лексики»[1] (составитель Леонов А.П., 2002 .), Русско-английский глоссарий по информационному обществу — совместный проект Британского Совета в России, Института развития информационного общества и проекта «Российский портал развития» (авторский коллектив О.Н.Вершинская, Ю.Д.Волынский, Т.В.Ершова, Н.В.Кривошеин, А.С.Мендкович, М.В.Моисеева, С.А.Нехаев, Г.Л.Смолян, Ю.Е.Хохлов, Д.С.Черешкин, С.Б.Шапошник), приложения к работам Стрельцова А.А., Федорова А.В. и других авторов.

Автоматизированная система
система программных и аппаратных средств, предназначенных для автоматизации процесса деятельности человека. В отличие от автоматической системы А.с. всегда функционирует при участии человека.

Автоматическая система
система программных и аппаратных средств, функционирующих самостоятельно, без участия человека.

Автор программы для ЭВМ или базы данных
Физическое лицо, в результате творческой деятельности которого они созданы.

Авторизация
предоставление прав, которое включает предоставление доступа, основанное на правах доступа. Процесс проверки имеющихся у пользователя прав и разрешений на доступ к ресурсу. Предоставление пользователю определенных полномочий на выполнение некоторых работ в вычислительной системе.

Администратор базы данных
человек или группа лиц, ответственные за состояние, развитие и использование базы данных организации или учреждения. А.б.д. обеспечивает работоспособность базы дан-

[1] http://morepc.ru/informatisation/leonov.html

ных, контролирует и поддерживает полноту, правильность, непротиворечивость и целостность данных, необходимый уровень защиты данных. Он взаимодействует с пользователями и программистами, программы которых используют доступ к базе данных.

Администратор безопасности

ответственное должностное лицо, уполномоченное установленным порядком на проведение работ в области защиты информации и поддержание уровня защиты объекта информатизации (сети передачи данных) и его ресурсов на этапах промышленной эксплуатации данного объекта информатизации (сети передачи данных) в установленном штатном режиме работы.

Адрес IP

числовой адрес компьютера в вычислительной сети, построенной на протоколах IP, например Интернет. Передача данных в такой сети возможна только по адресам IP. На данный момент используется 32-битная адресация, позволяющая использовать до 4 млрд различных адресов. Отдельные диапазоны адресного пространства обрабатываются особо: например, «петля обратной связи» (loopback) для передачи информации самому себе, блоки адресов для использования в локальных вычислительных сетях, адреса для широковещательной рассылки (broadcast) и групповой трансляции (multicast). При записи 32-битного адреса его байты разделяются точками, например: 192.168.38.94 (адрес 3'232'245'342 или $C0A8265E_{16}$). Для увеличения адресного пространства планируется ввести 128-битную адресацию, которая позволит свободно выделять адреса для многих устройств в сети. Поскольку числовой адрес неудобен для запоминания человеком, была разработана специальная система доменных имен, позволяющая назначить одному компьютеру одно или несколько словесных обозначений.

Антивирусная программа

программа, созданная, чтобы выявлять вирусы и, возможно, чтобы предложить или предпринять корректирующее действие. Обслуживающая программа, предназначенная для поиска, диагностики, профилактики и «лечения» файлов, зараженных компьютерным вирусом. В процессе поиска и диагностики определяются зараженные файлы и тип вируса. Профилактика позволяет предотвратить заражение. Например, резидентная А.п. предотвращает несанкционированное пользователем изменение файлов операционной системы, запись в сектор начальной загрузки и т.п. Лечение — это удаление вируса, восстановление файлов и т.п.

Аппаратная закладка

специальное электронное устройство перехвата информации, скрытно встраиваемое илиподключаемое к техническим средствам объекта информатизации (сети передачи данных) в целях несанкционированного получения защищаемой информации).

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 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, содержащих конкретный пароль).

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.

Аутентификация
положительная процедура установления пользователя, устройства или другого активного элемента в *информсистеме* по его заявленным полномочиям и паролю, иногда с использованием других, в т.ч. биометрических характеристик или предъявляемых электронных ключей.

Безопасности информационной обеспечение
система мер и норм, нацеленная на поддержание *безопасности информационной*. Осуществляется по следующим направлениям: *организационное, нормативно-правовое, технологическое* и *кадровое*. В составе системы обеспечения *безопасности информационной* могут создаваться подсистемы (системы), ориентированные на решение задач по отдельным направлениям обеспечения *безопасности информационной*. Система обеспечения *безопасности информационной* государства является частью системы обеспечения его национальной безопасности.

Безопасности информационной системы нарушение (акции)
нарушение средств управления специфической частью *системы информационной,* отвечающей за контроль *целостности информации* и доступа к системе. Может быть как преднамеренное в результате неправомерных действий *злоумышленника,* так и в результате сбоя в работе отдельных программ или технических компонентов системы. В любом случае следствием является облегчение доступа к информации или *информации нарушение* в результате неверной (неконтролируемой) работы программного обеспечения защиты данных от изменений.

Безопасности информационной угроза
фактор или совокупность факторов, создающих опасность функционированию, сохранению и развитию *пространства информационного*.

Безопасность
1) меры, принимаемые для защиты от всех действий, разработанных (предназначенных) для нанесения ущерба или снижения эффективности функционирования объекта или системы;
2) состояние, которое следует из внедрения и применения мер, которые гарантируют защиту от противоправных действий или влияний.

Безопасность информационная
1) состояние защищенности основных интересов личности, общества и государства в *пространстве информационном,* включая *инфраструктуру информационно-телекоммуникационную* и собственно *информацию* в отношении таких ее свойств, как *целостность, объективность, доступность* и *конфиденциальность;*
2) совокупное состояние:
— *пространства информационного,* при котором обеспечивается его формирование и развитие в интересах граждан, организаций и государства,
— *инфраструктуры информационной,* при котором информация используется строго по назначению и не оказывает негативного воздействия на систему (объект) при ее использовании,

— *информации,* при котором исключается или существенно затрудняется нарушение таких ее свойств, как *конфиденциальность*, *целостность* и *доступность;*
3) защищенность информационной среды личности, общества и государства от преднамеренных и непреднамеренных угроз и воздействий.

Безопасность информационная международная
состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в *пространстве информационном*.

Безопасность коммуникаций
защита (состояние защищенности), основанная на реализации совокупности разработанных (предназначенных) мер, предотвращающая *доступ неправомочный* к коммуникациям, а также исключающая *неправомерное использование информации,* в них циркулирующей, в любых целях. Включает как компоненты защиту *средств передачи данных технических* и защиту передаваемых данных, в том числе *криптозащиту.*

Безопасность компьютерная (Безопасность систем информационная)
защита АИС с использованием мер и средств (организационных и программно-технических), которые гарантируют *конфиденциальность, целостность* и *пригодность* информации, хранимой и обрабатываемой с использованием компьютерных средств; они включают технологию, процедуры и аппаратные средства ЭВМ и компоненты программного обеспечения, необходимые для защиты систем вычислительных комплексов и информации, обрабатываемой, хранимой и передаваемой как внутри системы, так и от нее к другим информационно-вычислительным системам.

Бета-тестирование
пробная эксплуатация программного продукта перед его выпуском на рынок. В процессе Б.-т. выявляются ошибки, связанные с непосредственным использованием продукта и не замеченные при разработке и испытаниях. По результатам Б.-т. фирма-разработчик корректирует программный продукт, после чего он тиражируется и поступает на рынок.

Биометрический
относящийся к использованию особых атрибутов, отражающих такие уникальные личные характеристики, как отпечаток пальца, рисунок кровеносных сосудов глаза, запись голоса, позволяющих идентифицировать лицо.

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.*

Вандал
в отличие от *кракера* и *хакера* этот термин используется в отношении действующих в *киберпространстве злоумышленников,* ставящих целью своих акций уничтожение *массивов информационных* и/или *систем информационных.* Их особенностью можно считать то, что они исходят из того, что противник знает об их *нападении.* Возможно, это определяется тем, что их целями являются специфические организации.

Взрыв информационный
резкий количественный и качественный скачек в сфере информации и коммуникации, вызванный научно-техническим процессом.

Виртуальное поле боя
применяется в военном контексте как эфир, занятый импульсами коммуникаций, базами данных, компьютерными сообщениями. В этом использовании синонимичен *киберсреде, киберпространству, инфосфере.*

Вирус программный
обобщенный термин, определяющий фрагмент программного кода, способный самокопироваться («размножаться») путем записи своей копии в коды других программ компьютерной системы, подвергающейся компьютерному проникновению, разработанный для негативного воздействия на информацию или программное обеспечения 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.

Вмешательство в информационно-телекоммуникационные системы и информационные ресурсы несанкционированное
вмешательство в процессы сбора, обработки, накопления, хранения, отображения, поиска, распространения и использования информации с целью нарушения нормального функционирования систем или нарушение *целостности, конфиденциальности* и *доступности* информационных и телекоммуникационных ресурсов.

Воздействие информационное
акт применения *оружия информационного,* а также непосредственное воздействие на элементы *пространства информационного* противника иными методами с целью нанесения ущерба.

Воздействие информационное прямое
изменение или уничтожение информации противника без использования специальных информационных средств.

Воздействие информационно-психологическое

действия психологические, осуществляемые с прямым или опосредованным использованием *средств информационно-психологических.*

Воздействие информационно-энергетическое

воздействие на биосистемы, и прежде всего на человека, физических полей различной природы, модулированных семантическими (смысловыми) сигналами, воспринимаемое биологическими организмами, а также средой их обитания в форме сигналов, сообщений, сведений, образов (т.е. в виде информации).

Воздействие на информационное пространство силовое

нарушение с использованием *оружия информационного* нормального (установленного законными собственниками, владельцами и пользователями) функционирования *инфраструктуры общества информационной,* правил формирования, хранения и распространения информации и информационных ресурсов.

Воздействия информационного средства

1) совокупность специальных лингвистических, программных, технических и иных средств, обеспечивающих извлечение, искажение или разрушение *информации, потоков информационных* или *ресурсов информационных;*

2) в информационных операциях эффективное использование *информации, систем информационных* и технологий в целях усиления средств и сил при осуществлении стратегии *операций информационных.*

Война 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:*

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.

Подавление и уничтожение систем управления противоборствующей стороны — направлено на физическое уничтожение командных пунктов противника, нарушение управления его силами и средствами.

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.

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.

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.

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.

Кибернетическая война — имеет целью нанесение ущерба информационным ресурсам противоборствующей стороны. Эта разновидность насильственных действий может быть реализована в виде:

информационного терроризма, проявляющегося в виде разрозненных случаев насилия в отношении специально выбранных целей;

информационных атак, направленных на изменение алгоритмов работы информационных систем при сохранении видимости нормального функционирования;

демонстрации силы, направленной на внушение противоборствующей стороне требуемого представления о возможных последствиях применения против нее того или иного оружия;

виртуализации реального мира.

Война информационная косвенная

изменение информации противника, создание явлений, которые противник должен наблюдать, анализировать и учитывать в своих стратегических и тактических действиях.

Война информационная экономическая

применение тактики войны информационной к основным процессам в экономическом пространстве.

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

позиционирования (GPS), сеть навигационных спутников, наземные/бортовые навигационные приборы.

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.

Восприятие

процесс отражения действительности в форме чувственного образа объекта, иначе — процесс оценки *информации,* которая была получена и классифицирована пятью физическими чувствами (зрение, слух, обоняние, вкус и осязание) и интерпретировалась в соответствии с критериями культуры и общества.

Восприятием управление

в данном контексте следует относить к методам *воздействия информационно-психологического.* Действия, сводящиеся к передаче или селектированию *информации* и индикаторов восприятия и имеющие целью влиять на эмоции, поводы и объективное рассуждение субъектов восприятия. Нацелено, в первую очередь, на интеллектуальную элиту общества страны противника и лидеров всех уровней с тем, чтобы влиять на официальные оценки, в конечном счете заканчивающиеся официальными действиями, благоприятными целям субъекта *восприятием управления*. Различными способами *восприятием управление* комбинирует проектирование правды, безопасность действий, сокрытие и обман, а также специальные психологические действия.

Вторжение

в данном контексте — *доступ неправомочный* или *проникновение* любого рода (физическое или информационное) в компьютеры, информационные системы и сети непосредственно или опосредованно через корреспондирующие сети или системы.

Вторжение электромагнитное

намеренное воздействие электромагнитной энергией на процессы обработки или передачи информации любым способом с целью их нарушения, изменения, в том числе изменения или нарушения обрабатываемой или передаваемой информации, обмана операторов или внесения беспорядка в организационные структуры обработки и передачи информации. Может являться элементом *войны радиоэлектронной*.

Вторжения обнаружение

1) фиксация факта *вторжения,* в том числе *вторжения электромагнитного* по каким-либо признакам;

2) процесс (действия) определения признаков, дающих основание сделать заключение о совершении *вторжения,* в том числе *вторжения электромагнитного.*

Вторжения обнаружения система

программное обеспечение и/или система аппаратных средств ЭВМ, разработанная (предназначенная) для контроля технико-программных средств компьютера, информационной системы или сети с целью идентификации признаков *вторжения попытки.*

Вторжения попытка

действия, направленные на осуществление *вторжения,* однако по какой-либо причине не завершенные или не приведшие к собственно *вторжению.* Однако уже на этом этане может представлять опасность и привести к нежелательным последствиям в зависимости от использовавшихся методов и стадии завершенности *вторжения попытки.*

Гарантия информационная

1) мера уверенности (доверия), что особенности системы безопасности (проводимые акции) и архитектура информационной системы (сети) точно отражают и обеспечивают принятую политику безопасности системы (сети);

2) *операции информационные оборонительные,* которые охраняют и защищают информацию и *системы информационные,* обеспечивая их *доступность, целостность, достоверность, конфиденциальность* и невозможность ее отрицания. Сюда относится обеспечение восстановления информационных систем с помощью привлечения возможностей по защите, обнаружению и реагированию.

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 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:

- создание механизмов государственного управления деятельностью в области защиты информации;

- развитие законодательства в сфере защиты информации;
- защита государственных информационных ресурсов;
- создание условий для развития рынка современных технологий и услуг по защите информации;
- 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);
- 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 инфообществу.

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 (см.: *спуфинг)*.

Данные

в данном контексте: 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.

Данные — управляемое нападение

форма нападения *(атака),* при котором агрессивный программный блок внедряется в форме внешне безвредных данных, подготовленных от имени официального пользователя или в ходе штатной работы программного обеспечения, что позволяет преодолевать защитные системы информационных сетей типа *фаэвол* и начинать атаку против поражаемой системы уже «позади» *фаэвол*.

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 неправомочные
действия в отношении *информресурса,* совершаемые в нарушение правил и полномочий (санкций), установленных для данного ресурса.

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 объекг 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.

Доминирование информационное
подавляющее преимущество, полученное через превышающую эффективность информационной деятельности (приобретение и использование данных, информации, знаний) в такой степени, что это преимущество демонстрируется практически через превышающую эффективность инструментальной деятельности.

Доступ контрактный
преднамеренное указание неверных данных при заключении контракта или невыполнение абонентом информационной сети или сети связи контрактных условий оплаты.

Доступ несанкционированный (неправомочный)
доступ к *ресурсу информационному,* совершаемый в нарушение правил и полномочий (санкций), установленных для данного ресурса.

Доступ ограниченный
доступ к *ресурсу информационному,* разрешаемый только определенному установленными для данного ресурса правилами и полномочиями (санкциями) кругу лиц.

Доступ неправомерный как вид мошенничества
несанкционированное использование услуг связи, неправомочный и преднамеренный доступ абонента к услугам связи с целью личной или коллективной выгоды.

Доступ технический
неправомочное изготовление (клонирование) телефонных трубок или платежных телефонных карт с фальшивыми идентификаторами абонентов, номеров и платежных отметок.

Доступ фрикерский
проникновение в телекоммуникационную сеть для получения информации обмена кодами доступа, их изменения и использования в своих целях, взлом системы защиты.

Доступа несанкционированного предпосылки
совокупность факторов, создающих благоприятные условия для *доступа несанкционированного*.

Доступность
характеристика информации, определяющая возможность ее получения пользователем информационной системы. Выделяют *информацию открытую* и *информацию ограниченного доступа*.

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.

Зашиты информации системы
система мер и действий, направленных на обеспечение *информации безопасности с* использованием всех возможностей *защиты информации инфраструктуры*.

Защита информационная
совокупность информационных средств, обеспечивающих (предназначенных для) противодействие *воздействию информационному,* включая *атаки информационные,* а также реализуемым на каналах распространения информации (СМИ, сети передачи данных и т.п.) *действиям психологическим*.

Защита радиоэлектронная
раздел РЭБ, включающий действия, предпринимаемые для защиты личного состава, объектов и оборудования от любых последствий применения средств РЭБ своими войсками или противником, ведущих к снижению эффективности, нейтрализации или уничтожению боевых возможностей своих войск.

Защиты информации инфраструктура
разделенная или связанная совокупность компьютеров, коммуникаций, данных, технологий и систем безопасности, систем обучения, обеспечения, использования и подготовки кадров и других структур поддержки всех форм *безопасности информации* и информационных инфраструктур всех уровней для данного объекта, структуры, территории.

Идентификация
процедура проверки идентичности пользователя, устройства или другого активного элемента в *системе информационной* в соответствии с его фактическими и заявленными полномочиями и парольной системой (иногда с использованием других, в частности биометрических характеристик), часто рассматривается как условие разрешения доступа к ресурсам в системе.

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 источни-

ком 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.

Информатизации средства

технические, программные, лингвистические, правовые, организационные средства (средства вычислительной, множительной и пр. предназначенной для обработки и размножения информации и информационных материалов техники, компьютерные программы, словари, тезаурусы и классификаторы, инструкции и методики, положения, уставы, должностные инструкции, эксплуатационная и сопроводительная документация), используемые или специально создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

Информатизация

организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов. Процесс интенсификации производства и распространения знаний и информации, основанный на использовании информационно-коммуникационных технологий (ИКТ).

Информатика, компьютерная наука

научное направление, изучающее свойства информации и способы ее представления, накапливания, автоматической обработки и передачи. И. начала формироваться в начале 70-х гг. как дополнение и конкретизация кибернетики в связи с использованием ЭВМ в управлении, науке, проектировании, образовании, сфере услуг и т.д. В И. входит группа дисциплин, занимающихся различными вопросами, связанными с разработкой и применением вычислительной техники: прикладная математика, программирование, искусственный интеллект, архитектура ЭВМ, вычислительные сети и др. Современная прикладная И. занимается специальными информационными системами, основанными на ЭВМ и реализующими машинные информационные технологии. Эти системы подразделяются на управленческие, административные, исследовательские, учебные, проектирующие, коммуникационные, системы обслуживания бытовой сферы, экологические, медицинские, военные и т.д. И. охватывает все аспекты их разработки, внедрения и влияния на развитие общества.

Информации разрушение

полная потеря хранящихся в информационных системах или передаваемых по информационным сетям данных или их изменение, исключающее возможность правильной их интерпретации и восстановления.

Информации утечка

совершившийся факт разглашения (распространения) *информации ограниченного доступа* за пределами санкционированного круга лиц в результате совершенных *действий неправомочных*.

Информации уязвимость

свойство хранимых, обрабатываемых и передаваемых данных, массивов и документов, при котором имеется потенциальная возможность их утечки, физического разрушения и несанкционированного использования

Информационная инфраструктура

система формирования, распространения и использования *информационных ресурсов*, включая рынок *информационных услуг* и средств массовой информации. Совокупность организационных структур, которые обеспечивают функционирование и развитие информационного пространства страны, а также средств информаци-

онного взаимодействия, обеспечивающих доступ граждан и организаций к информационным ресурсам. Часть структуры информационного пространства, которая обеспечивает создание и циркуляцию *информационных потоков* в пространстве. Основные характеристики информационной инфраструктуры: качественный и количественный состав элементов инфраструктуры; пространственное расположение элементов и их взаимосвязь; информационная производительность и пропускная способность элементов и всей информационной инфраструктуры в целом. Основные элементы информационной инфраструктуры: телекоммуникации; *информационные сети*; информационные ресурсы; системы информационного обслуживания. Дополнительные (вспомогательные элементы): системы обеспечения развития и функционирования информационной инфраструктуры.

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 негативных информационно-психологических воздействий.

Информационные продукты

документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей. *Информационные ресурсы* всех видов, программные продукты, базы и банки данных и другая информация, представленные в форме товара. Совокупность данных, подготовленная производителем для последующего распространения в вещественной документальной или электронной форме в качестве товара или услуги. Информация, представляющая собой результат деятельности какого-либо лица.

Информационный продукт включает: информацию (данные, знания); носители информации; информационные средства и технику; продукты, обеспечивающие информационную деятельность.

Информационные процессы

процессы создания, сбора, обработки, накопления, хранения, отображения, передачи, поиска, распространения и потребления информации.

Информационные ресурсы

отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах) .

Информационные услуги

информационная деятельность по доведению до пользователя информационной продукции, проводимая в определенной форме.

Информационный бизнес

направление деловой активности общества, связанное с реализацией функций торговли и посредничества на информационном рынке, а также организацией производства, обслуживания, аренды, страхования, финансового и кадрового обеспечения средств массовой информатизации общества.

Информационный город

город, обладающий постиндустриальной инфраструктурой экономики, в котором главными сферами деятельности являются управление, финансовая деятельность, научные исследования, высшее образование, культура, информационное обслуживание, СМИ, деловые услуги (рекламные, консалтинговые, информационные и т. п.), причем в этих видах деятельности занято более половины всех работающих.

Информационный криминал
преднамеренные злоумышленные действия, направленные на хищение или разрушение информации в информационных системах и сетях, исходящие из корыстных или хулиганских побуждений.

Информационный объект
компьютерная или телекоммуникационная система, одно или совокупность аппаратных и (или) технических средств обработки информации, помещение, в котором установлены система или средства обработки и (или) передачи информации или ведутся конфиденциальные переговоры.

Информационный посредник
лицо, которое от имени другого лица отправляет, получает или хранит электронные документы или предоставляет другие услуги в отношении данных документов.

Информационный потенциал общества
совокупность средств, методов и условий, позволяющих активизировать и эффективно использовать информационные ресурсы, способность производить информацию и оказывать информационные услуги.

Информационный поток
перемещаемая в пространстве и времени информация.

Информационный рынок
система экономических, правовых и организационных отношений в обществе, которая обеспечивает торговлю средствами информационной техники, информационными технологиями, информационными продуктами, а также предоставление на коммерческой основе информационных услуг пользователям.

Информационный товар
информационный продукт, произведенный для обмена или продажи; *информационная услуга* как предмет продажи; товар, обеспечивающий информационную деятельность (информационные средства и техника, произведенные для продажи).

Информация о гражданах (персональные данные)
сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Информации защита
совокупность организационных, правовых, технических и технологических мер по предотвращению и отражению угроз *ресурсам информационным* и *системам информационным,* устранению их последствий.

Информация
1) сообщение, осведомление о положении дел, сведения о чем-либо, передаваемые людьми;
2) уменьшаемая, снимаемая неопределенность в результате получения сообщений;
3) сообщение, неразрывно связанное с управлением, сигналы в единстве синтаксических, семантических и прагматических характеристик;
4) передача, отражение разнообразия в любых объектах и процессах (неживой и живой природы);
5) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы предоставления.

Информация бытовая
сведения, возникающие в процессе обыденного человеческого общения.

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 ограниченного доступа
вид сведений, доступ к которым ограничен в соответствии с законодательством и разглашение которых может нанести ущерб интересам других лиц, общества и государства. В составе такой информации различают сведения, составляющие государственную тайну, и *информацию конфиденциальную.*

Информация открытая
общедоступные сведения, не имеющие ограничений по доступу к ним всех заинтересованных лиц.

Информация развлекательная
сведения, предназначенные для использования человеком в основном в процессе отдыха. К информации такого рода следует отнести прежде всего произведения художественной литературы, концертные программы, кинофильмы, телепередачи и т.д.

Информация распорядительная
сведения, возникающие в связи с реализацией человеком некоторых нормативных предписаний, инструкций: заполнение служебных журналов, управление движением автотранспорта, производственным станом и пр.

Информация служебная
сведения, появляющиеся в связи с реализацией функций государственной службы. Круг сведений, составляющих *информацию служебную,* весьма широк и охватывает все сферы деятельности органов государственной власти.

Информация социально-значимая
сведения об интересующих значительное количество людей событиях общественной жизни внутри страны и за рубежом, деятельности политических партий и движений, лидеров общества и государства, рынке труда и капитала и т.д., кроме некоторых наиболее общих сведений о состоянии экономической сферы.

Информация частная
сведения, раскрывающие реализацию гражданином своих личных конституционных прав на свободу мысли, совести, собраний, информационной деятельности, о его мировоззрении, нравственных *ценностях,* отношении к религии и т.д. Как правило, затрагивает ограниченный круг лиц и касается их частной жизни.

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
технические средства и системы формирования, обработки, хранения и передачи информации. Является средой, которая обеспечивает возможность сбора, передачи, хранения, автоматизированной обработки и распространения информации в обществе.

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.

Инфраструктура информационная национальная
единая или взаимосвязанная система компьютерной техники, линий связи, использования данных, безопасности, личного состава, обучения и других вспомогательных структур, обслуживающих местные, национальные и всемирные информационные нужды и функционирующих в интересах и масштабах государства.

Инфраструктура информационная общества
совокупность *систем информационно-телекоммуникационных* и *связи сетей,* индустрии средств информатизации, телекоммуникации и связи; системы формирования и обеспечения сохранности информационных ресурсов; системы обеспечения доступа к *средствам информационно-телекоммуникационным, связи, сетям* и *ресурсам информационным; информационных услуг индустрии* и *рынка информационного* системы подготовки и переподготовки кадров, проведения научных исследований.

Инцидент
при проведении информационных операций — проанализированный случай попытки получения *доступа несанкционированного* или *нападения информационного* на автоматизированную информационную систему. Он включает несанкционированное зондирование и просматривание; прерывание или воспрещение обслуживания; искаженный или уничтоженный ввод, обработку, хранение или вывод информации, внесение изменений в характеристики аппаратного оборудования, программно-аппаратных средств или программного обеспечения информационной системы с (или без) ведома, инструкции или намерения пользователя.

Искусственный интеллект, машинный интеллект
область, которая рассматривается как часть науки о компьютерах, связанная с моделированием и системами, реализующими функции, такие как рассуждение и обучение, обычно ассоциируемые с человеческим интеллектом. Область информатики, занимающаяся научными исследованиями и разработкой методов и средств для правдоподобной имитации отдельных функций человеческого интеллекта с помощью автоматизированных систем. В рамках И. и. создаются методы, программные и технические средства решения задач, для которых отсутствуют формальные алгоритмы: распознавание изображений, понимание естественных языков и речи, обучение с учетом способностей ученика, постановка диагнозов, доказательство теорем и т. п. Эти задачи обычно решаются человеком с привлечением подсознания и поэтому их довольно трудно моделировать. На основе методов И. и. разрабатываются программные интеллектуальные системы, например, интеллектуальные информационные системы, интеллектуальные обучающие системы, интеллектуальные системы программирования и др. Большинство таких систем используют для своей работы соответствующие базы знаний, которые также разрабатываются с привлечением методов И.и. Иногда про-

граммы И.и. служат для моделирования поведения человека, а иногда — для технических применений. Методы И.и. помогают и в программировании компью-терных игр. Термин «машинный интеллект», являясь синонимом И.и., чаще служит для указания только технологического аспекта проблемы И.и. Свойство автоматических и автоматизированных систем выполнять отдельные функции интеллекта человека, например выбирать и принимать оптимальные решения на основе ранее полученного опыта и анализа внешних воздействий.

Использование информации неправомерное

передача, распространение (публикация), применение в *действиях информационных* полученных легальным путем сведений в нарушение правил и полномочий (санкций), установленных для данных сведений и субъекта, предпринявшего такие действия.

Использование ИТКС и информресурсов неправомерное

использование без соответствующих прав или с нарушением установленных правил, законодательства или норм международного права.

Кодификатор (классификатор) компьютерных преступлений

разработан в 1991 г. рабочей группой Интерпола. К. к. п. интегрирован в автоматизированную систему поиска информации по запросам и в настоящее время доступен Национальным бюро Интерпола более чем 100 стран. К. к. п. содержит шесть групп компьютерных преступлений, каждая из которых разбита на отдельные виды. В К. к. п. предусмотрена опция Z, обозначающая «прочие виды преступлений» и предназначенная для учета возможного развития компьютерных технологий.

- Группа QA — Несанкционированный доступ и перехват:

— QAH — *компьютерный абордаж (хакинг)*: несанкционированный доступ в компьютер или компьютерную сеть;

— QAI — *перехват*: несанкционированный перехват информации при помощи технических средств, несанкционированные обращения в компьютерную систему или сеть как из нее, так и внутри компьютерной системы или сети;

— QAT — *кража времени*: незаконное использование компьютерной системы или сети с намерением неуплаты;

— QAZ — прочие виды несанкционированного доступа и перехвата.

- Группа QD — Изменение компьютерных данных:

— QDL — *логическая бомба*: неправомерное изменение компьютерных данных путем внедрения логической бомбы;

— QDT — *троянский конь*: неправомерное изменение компьютерных данных путем внедрения троянского коня;

— QDV — *вирус*: изменение компьютерных данных или программ без права на то, путем внедрения или распространения компьютерного вируса;

— QDW — *червь*: несанкционированное изменение компьютерных данных или программ путем передачи, внедрения или распространения компьютерного червя в компьютерную сеть;

— QDZ — прочие виды изменения данных.

- Группа QF — Компьютерное мошенничество:

— QFC — *компьютерные мошенничества с банкоматами*: мошенничества, связанные с хищением наличных денег из банкоматов;

— QFF — *компьютерные подделки*: мошенничества и хищения из компьютерных систем путем создания поддельных устройств (карточек и пр.).

— QFG — *мошенничества с игровыми автоматами*: мошенничества и хищения, связанные с игровыми автоматами;

— QFM — *манипуляции с программами ввода-вывода*: мошенничества и хищения посредством неверного ввода или вывода в компьютерные системы или из них путем манипуляции программами;
— QFP — *компьютерные мошенничества с платежными средствами*: мошенничества и хищения, связанные с платежными средствами;
— QFT — *телефонное мошенничество*: доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы;
— QFZ — прочие компьютерные мошенничества.

- Группа QR — Незаконное копирование:

— QRG/QRS — *незаконное копирование*, распространение или опубликование компьютерных игр и другого программного обеспечения;
— QRT — *незаконное копирование топологии полупроводниковых изделий*: незаконное копирование защищенной законом топологии полупроводниковых изделий или незаконная коммерческая эксплуатация или импорт с этой целью топологии или самого полупроводникового изделия, произведенного с использованием данной топологии;
— QRZ — прочее незаконное копирование.

- Группа QS — Компьютерный саботаж:

— QSH — *саботаж с использованием аппаратного обеспечения*: ввод, изменение, стирание или подавление компьютерных данных или программ или вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы;
— QSS — *компьютерный саботаж программы*: несанкционированное стирание, повреждение, ухудшение или подавление компьютерных данных или программ;
— QSZ — прочие виды саботажа.

- Группа QZ — Прочие компьютерные преступления:

— QZB — *электронные доски объявлений (BBS)*: использование BBS для хранения, обмена и распространения материалов, имеющих отношение к преступной деятельности;
— QZE — *хищение информации, представляющей коммерческую тайну (компьютерный шпионаж)*: приобретение незаконными средствами или передача информации, представляющей коммерческую тайну без права на то или другого законного обоснования, с намерением причинить экономический ущерб или получить незаконные экономические преимущества;
— QZS — *материал конфиденциального характера*: использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера;
— QZZ — прочие компьютерные преступления.

Коммерческая информация

информация, распространяемая только по желанию ее обладателя и на его условиях; объект купли-продажи.

Коммерческая тайна

сведения конфиденциального характера из любой сферы деятельности государственного или частного предприятия, разглашение которых может нанести материальный или моральный ущерб ее владельцам или пользователям (юридическим лицам). Охрана коммерческой тайны осуществляется ее владельцем. Информация, составляющая управленческую, производственную, научно-техническую, кредитно-финансовую, торговую и иную деловую информацию, а также содержащая специально охраняемые сведения, в том числе секреты производства, может быть закрыта как коммерческая тайна. Информация, охраняемая как коммерческая тайна, должна соответствовать следующим требованиям:

- иметь действительную или потенциальную ценность;
- не являться общеизвестной или общедоступной;
- обозначаться соответствующим образом с осуществлением правообладателем надлежащих мер по сохранению ее конфиденциальности через установление соответствующего правового режима, включающего правила закрытия сведений, введение соответствующей маркировки документов и иных носителей информации, организации конфиденциального делопроизводства;
- не являться государственным секретом и не защищаться авторским или патентным правом;
- не касаться негативной деятельности субъекта хозяйствования, способной нанести ущерб интересам государства.

Информация, охраняемая как коммерческая тайна, не может включать:

- учредительные документы, а также документы, свидетельствующие о праве субъекта на занятие предпринимательской деятельностью и отдельными видами хозяйственной деятельности;
- сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные данные, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей;
- документы о платежеспособности;
- сведения о численности и составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест.

Содержание и объем информации, охраняемой как коммерческая тайна, а также порядок ее защиты определяются руководителем субъекта хозяйствования, который доводит их до работников либо лиц, имеющих доступ к таким сведениям.

Один из объектов гражданских прав, предусмотренных ГК РФ, с особым режимом защиты. Согласно ст. 139 ГК РФ информация составляет К. т. в случае, когда она имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять К. т., определяются законом и иными правовыми актами. Информация, составляющая К. т., защищается способами, предусмотренными ГК РФ и другими законами. Лица, незаконными методами получившие информацию, которая составляет К. т., обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших К.т. вопреки трудовому договору, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Капля

«двоичный большой объект», используемый для описания любой случайной большой совокупности частиц, обычно картина или звуковой файл. Нередко используется как умеренная угроза хакера при отправлении по электронной почте *(бомба почтовая)*. Может также использоваться, чтобы скрыть *бомбу логическую*.

Киберпространство

наиболее часто употребляемый из ряда синонимов, к которым следует отнести термины типа: *киберсреда, инфосфера,* а также чисто англоязычный datasphere.

Кибертерроризм

синоним: *терроризм информационный*.

Командования и управления боевое применение

комплексное использование мер обеспечения секретности операций, военной дезинформации, психологических операций, средств РЭБ и физического уничтожения при взаимной поддержке разведки в целях не допустить разглашения информации, оказать влияние, снизить эффективность или уничтожить средства командования и

управления противника, в то же время осуществляя защиту своих средств командования и управления против таких действий. Боевое применение командования и управления представляет собой использование информационных операций. Бывает как наступательным, так и оборонительным.

Командования и управления система, атака

синхронизированное выполнение действий, направленных на снижение эффективности функционирования *командования и управления системы,* воздействуя на информацию и информационные системы и сети противника.

Командования и управления система, средства воздействия

средства информационного воздействия, психологических действий, радиоэлектронной войны и физического разрушения, направленные на деградацию или уничтожение *командования и управления системы* противника, при защите своей аналогичной системы против таких действий. Применение данных средств может рассматриваться как часть *войны информационной* в военных действиях. Могут применяться во все периоды военных действий и на всех уровнях конфликта.

Командования и управления системы защита

обеспечение эффективности *командования и управления системы* собственных сил при противодействии усилиям противника, направленным на ее деградацию или уничтожение. Система может носить наступательный или защитный характер: наступательные средства используют *командования и управления системы, средства воздействия,* чтобы уменьшить способность противника провести атаку; оборонительная составляющая уменьшает уязвимость своей системы для средств противника за счет применения адекватных физических, электронных и информационных мер и средств.

Контрдезинформация

усилия по воспрещению, нейтрализации, уменьшению последствий или по извлечению выгод из операций противника по *дезинформации*.

Контрмеры информационные

действия, устройства, процедуры, техника или другие меры, которые снижают уязвимость автоматизированной информационной системы или информационной сети. Контрмеры, которые нацелены на определенные угрозы и уязвимость, вовлекают более активные методы, такие как *безопасность* и *защита информационная*.

Контролируемый пакет

прием *атаки,* при котором нападавшие тайно вставляют программу в отдаленных переключателях или хостах сети. Программа контролирует информационные пачки, посланные через сети, и посылает копию восстановленной информации *хакеру*. Анализируя полученные таким образом первые 125 символов связи, нападавшие могут изучать пароли и идентификаторы пользователя, которые, в свою очередь, они могут использовать, чтобы проникнуть в системы.

Конфиденциальность (информации)

принцип обработки, хранения и доступа к информации, обеспечивающий нераскрытие ее любому не уполномоченному на доступ к ней лицу. Частично синонимичен с тайной.

Кракер

термин, обозначающий любого, кто пытается проникнуть в информмассивы или сети за счет взлома их защиты, вне зависимости от цели проникновения.

Криптоанализ

1) раскрытие зашифрованного криптографическими методами текста с помощью известного ключа или без него (за счет вскрытия неизвестного ключа);

2) анализ криптографической системы и ее входных и выходных данных с целью определения засекреченных переменных и значимой информации, включая открытый текст.

Криптография

1) наука об использовании математических методов и технических средств для преобразования открытой защищаемой информации в закрытую, зашифрованную форму, затрудняющую восстановления открытой информации;

2) тайнопись, система изменения информации (текста, речи) с целью сделать ее непонятной для непосвященных лиц.

Криптология

наука о безопасности (секретности) передачи информации; включает *криптографию* (шифрование) и *криптоанализ.*

Люк

скрытое программное обеспечение или механизм аппаратных средств ЭВМ, позволяющие обходить контроль безопасности систем, в которых они функционируют. Синонимы: *задняя дверь, черный ход.*

Массив информационный

специальным образом организованная совокупность *информации документированной* или хранимой в электронном контуре *системы информационной.*

Модуль проверки текущего состояния

программный инструмент перехвата потенциально годных для использования данных в процессе их продвижения по информационной сети. Используется *хакерами,* чтобы захватить идентификатор и пароли пользователя.

Мошенничество компьютерное

компьютерное преступление, предусматривающее преднамеренное введение в заблуждение или изменение данных для получения незаконного дохода в любой форме и совершаемое через или в отношении компьютеров и/или информационных сетей.

Мусорщик

соумышленник, предпринимающий попытку по остаткам информационной деятельности восстановить чувствительные данные законного пользователя (идентифицирующие данные, пароли, сведения о полномочиях и т.п.) без его разрешения в целях последующего несанкционированного проникновения в систему под его именем. См.: *дампстер.*

Нападение

в данном контексте, акт, связанный с нанесением физического ущерба объекту *инфраструктуры информационной.*

Нападение на компьютерную сеть

операции, направленные на прерывание, воспрещение, снижение качества или уничтожение информации, находящейся в компьютерах или компьютерных сетях, или самих компьютеров и компьютерных сетей. Синоним: *атака.*

Нападение пассивное

нападение информационное, имеющее целью только открытие доступа к информации или информационным массивам без нанесения им прямого ущерба (изменения, уничтожения и пр.).

Нападение радиоэлектронное

раздел РЭБ, сопряженный с использованием электромагнитного оружия, *направленной энергии оружия* или оружия поражения излучающих радиоэлектронных систем для нападения на личный состав, объекты или оборудование с целью снижения эффективности, нейтрализации или уничтожения боевых возможностей противника. *Нападение радиоэлектронное* включает:

1) действия, предпринимаемые для предотвращения пли уменьшения эффективного использования противником электромагнитного спектра, такие как радиоэлектронное подавление и дезинформация с использованием радиоэлектронных

систем; 2) использование оружия, в котором применяется электромагнитная или направленная энергия в качестве основного поражающего механизма (лазеры, радиочастотное оружие, пучки направленной энергии или оружие поражения излучающих радиоэлектронных систем).

Нападение техническое

нападение, которое может быть совершено, обходя или аннулируя аппаратные средства ЭВМ и механизмы защиты программного обеспечения с использованием специальных аппаратных средств.

Напевать

преднамеренно отправлять по электронной почте провокационные сообщения с намерением отвлечь других и втянуть в бессмысленную переписку.

Направленной энергии оружие

система, использующая направленную энергию прежде всего непосредственно для повреждения или уничтожения основного оборудования, вооружений, средств их обеспечения и обслуживания и личного состава противника.

Нарушение средств безопасности системы

успешное поражение средства управления безопасностью, которое завершается проникновением в систему. Нарушение средств управления специфической информационной системы, как правило, приводит к тому, что информационные активы или компоненты системы становятся доступны неуполномоченным на то лицам или программно-техническим средствам.

Нарушитель

в данном контексте: лицо или группа лиц, совершающих *действия неправомочные* с использованием штатных техническо-программных средств.

НОРД-петля

«**н**аблюдение, **о**риентация, **р**ешение, **д**ействия петля». Общий принцип организации работы на основе информации. Нарушение или повреждение НОРД-петли — обычный способ теоретического описания цели и/или главного результата *воздействия*.

Обман

меры, разработанные (предназначенные), чтобы ввести в заблуждение противника манипуляцией, искажением или фальсификацией информации и тем самым стимулировать его реагировать способом, наносящим ущерб его интересам.

Обмен информационный международный

передача и получение информационных продуктов, а также оказание информационных услуг через государственную границу страны *ресурса информационного* владельца.

Обмена информационного международного средства

инфраструктура информационная, используемая при *обмене информационном международном*.

Обнаружение аномалии

обобщенный термин для класса тактик обнаружения *вторжения,* которые основаны на идентификации потенциальных *попыток вторжения* на основании их возможных аномальных по сравнению с ожидаемыми действий.

Общество информационное

1) состояние развития общественных и, прежде всего, производственных отношений, при котором основная часть валового продукта производится не за счет материального производства, а на основе создания и продажи наукоемких технологий, информационных продуктов, т.е. результатов интеллектуального труда граждан, а также самой информации, порождаемой в качестве продукта труда;

2) общество, в котором основным предметом труда большей или значительной части людей являются информация и знания, а орудием труда — информационные технологии.

Объективность (информации)

свойство информации, определяющее ее соответствие реальным описываемым с ее помощью объектам, процессам, явлениям.

Операции информационные

действия любого характера, предпринимаемые для оказания воздействия на информацию и информационные системы (сети) противника при защите своей собственной информации и информационных систем.

Операции информационные наступательные

единое использование приданных и поддерживающих возможностей и действий, поддерживаемых на взаимной основе разведкой, для оказания воздействия на руководство противника в целях достижения или развития конкретных задач. Эти возможности и действия включают, но не ограничиваются обеспечением секретности операций, военным введением в заблуждение, психологическими операциями, операциями РЭБ, физическим нападением и/или уничтожением и специальными информационными операциями, а также могут включать нападение на компьютерную сеть.

Операции информационные оборонительные

интеграция и координация политики, методик, операций, личного состава и технологии в целях охраны и защиты информации и информационных систем. Оборонительные информационные операции осуществляются посредством *гарантий информационных,* обеспечения физической безопасности, оперативной безопасности, *контрдезинформации,* контрпсихологических операций, контрразведки, РЭБ и *информационных операций специальных. Операции информационные оборонительные* обеспечивают своевременный, четкий и соответствующий доступ к информации, в то же время не давая противнику возможности использовать свою информацию и информационные системы в своих целях.

Операции информационные специальные

информационные операции, которые в силу своего секретного характера, их возможного потенциального эффекта или воздействия, соображений безопасности или угрозы национальной безопасности требуют особого процесса рассмотрения и одобрения.

Оружие информационное

1) средства и методы, применяемые с целью нанесения ущерба информационным ресурсам, процессам и системам государства, негативного информационного воздействия на оборонные, управленческие, политические, социальные, экономические и другие критически важные системы государства, а также массированной психологической обработки населения с целью дестабилизации общества и государства;

2) специальные средства, технологии и информация, позволяющие осуществить «силовое» воздействие на информационное пространство общества и привести к значительному ущербу политическим, оборонным, гномическим и другим жизненно важным интересам государства;

3) комплекс технических и других средств и технологий, предназначенных для:

— установления контроля над информационными ресурсами потенциального противника;

— вмешательства в работу его систем управления и информационных сетей, систем связи и т.п. в целях нарушения их работоспособности, вплоть до полного выведения из строя, изъятия, искажения содержащихся в них данных или направленного введения специальной информации;

— распространения выгодной информации и дезинформации в системе формирования общественного мнения и принятия решений;

— совокупность специальных способов и средств воздействия на сознание и психику политического и военного руководства, личного состава вооруженных сил, спецслужб и населения противостоящего государства, используемых для достижения превосходства в информационном противоборстве.

Оружие информационное стратегическое

совокупность видов *оружия информационного,* способного нанести неприемлемый ущерб политическим, экономическим и военным интересам страны, а также структурам, образующим ее стратегический потенциал, в рамках стратегической операции вооруженных сил государства.

Оружие информационное тактическое

совокупность видов *оружия информационного,* способного обеспечить решение важных задач в ходе боевых действий.

Отказ в обслуживании

действие, которое отстраняет любую часть информационной системы (сети) от функционирования в соответствии с предназначенной целью. Может включать отказ услуг или процессов, ограниченных одной машиной. Однако термин наиболее часто используется в контексте действий, хоть и направленных против одного абонента (пользователя), но которые приводят к неспособности исполнять функции по обслуживанию и других пользователей, особенно в рамках сети.

Отказ информационный средства, вызывающие

средства воздействия на информационные системы (сети) противника, приводящие к изменениям функций относительно целей системы. Имеются два типа такого воздействия: *нападение* на информсистемы противника и внедрение *дезинформации* в системы с целью стимулировать противника к невыгодным ему действиям. В военных условиях для прямых нападений используют средства РЭБ, «забивающие» радиосвязь и каналы передачи данных.

Пароля взламывание

техника тайно получать доступ к информсистеме (сети), в которой нападавшие пробуют угадать или украсть пароли. Пользователи часто выбирают слабый пароль. Два главных источника слабости в паролях — легко предполагаемые пароли, основанные на знании пользователя (например, девичья фамилия жены) и пароли, которые являются восприимчивыми к раскрытию с использованием словаря как источника предположений. Эта техника была легко автоматизирована *хакерами,* компьютеры могут очень эффективно и систематически делать предположение. Например, если пароль — слово словаря, компьютер может найти все возможности.

Пересмешник

компьютерная программа или процесс, который, имитируя стандартные программы или процессы вычислительного комплекса, исполняет злонамеренные действия в отношении данного комплекса или связанных с ним в рамках локальной сети.

Пигбекинг

получение *доступа неправомочного к* системе через законно установленную связь (доступ) другого пользователя.

Полномочия

в данном контексте — права пользователя по доступу к тем или иным ресурсам системы (сети) и на выполнение тех или иных действий в системе (сети). Задаются, как правило, идентификаторами и паролями. Практикуются различные системы идентификаторов, включая использующие данные биометрии и индивидуальные встраиваемые в личные документы микрочипы.

Пользователь

в данном контексте — лицо, использующее в своей служебной или частной деятельности *средства информационные* или *массивы информационные*.

Пользователь уполномоченный

пользователь, выступающий в системе или сети как представитель другого пользователя и пользующийся его правами *(пользователя полномочиями)* для выполнения каких-либо действий или доступа к информации.

Пользователя полномочия

права *пользователя* по доступу к *системе информационной,* обрабатываемой (хранимой) информации, конкретным технически-программным средствам или структурам информационной сети.

Право на закрытие охраняемой информации

собственник конфиденциальной информации имеет право на создание специальных условий, гарантирующих защиту такой информации, путем ее закрытия и организации охраны в соответствии с действующим законодательством. Конфиденциальная информация в зависимости от характера составляющих ее сведений может быть закрыта как:

- тайна личной жизни;
- профессиональная тайна;
- государственная и служебная тайны (государственный секрет);
- служебная информация ограниченного распространения;
- коммерческая тайна;
- банковская тайна .

Правовая информатика

наука, изучающая информацию, информационные процессы и информационные системы в праве (или в правовой системе). Объектами исследования в правовой информатике выступают:

- Информация в правовой системе как объект особого рода. Проводится классификация информации в правовой системе по разным основаниям. Изучаются особенности и юридические свойства информации; проблемы оценки количества и качества информации; роль информации в принятии юридических решений.
- Информационные процессы в правовой системе и возникающие при их осуществлении информационные отношения. Это процессы сбора, производства, распространения, преобразования, поиска, получения, передачи и потребления информации. Существенное внимание правовая информатика обращает на изучение общественных отношений, возникающих в информационных процессах, на особенности этих отношений, вызываемых юридическими свойствами информации.
- Информационные системы, информационно-телекоммуникационные технологии и средства их обеспечения, в том числе автоматизированные информационные системы, базы и банки данных, их сети, другие информационные технологии, используемые для правовых целей, создаваемые на основе средств вычислительной техники, связи и телекоммуникаций.

Превосходство информационное

степень доминирования в информобласти, которая разрешает проведение действий без опасности эффективного противодействия.

В военной трактовке: возможность сбора, обработки и распространения непрерывного потока информации, в то же время используя в своих целях или не давая возможности противнику делать то же самое.

Преступление компьютерное

преднамеренная или иная *деятельность неправомочная,* которая воздействует *на пригодность, конфиденциальность,* или *целостность* информационных или иных

ресурсов с использованием компьютерных средств. *Преступление компьютерное* может включать мошенничество, растрату, воровство, злонамеренное повреждение, неправомочное использование, отказ или изменение порядка обслуживания и незаконное присвоение.

Преступность информационная международная
использование ИТКС и ресурсов и воздействие на такие системы и ресурсы в международном информационном пространстве в противоправных целях.

Пригодность (готовность) информации
обеспечение способностей системы продолжать работать эффективно и поддерживать доступность информации. Принцип, который гарантирует, что система и данные работают и доступны пользователям. Отказ от обслуживания рассматривается как нападение на пригодность информации.

Приемлемый уровень риска
разумная и тщательно рассматриваемая оценка достаточности соответствующей системы защиты минимальным требованиям применяемых директив безопасности. Оценка должна учитывать ценность активов системы, реальные и гипотетические угрозы и практическую уязвимость системы, возможные контрмеры и эксплуатационные требования.

Проба
в информационных операциях любая попытка получения информации об автоматизированных информационных системах или их пользователях, работающих в диалоговом режиме (онлайн).

Продукт информационный
документированная или передаваемая по электронным каналам связи информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей.

Проникновение
в данном контексте: успешная *атака* — приобретение способности получить неправомочный и необнаруженный доступ к файлам и программам или системе управления информационной системы (сети). Успешный акт обхода механизмов обеспечения безопасности, неправомочный доступ к информационной системе (сети).

Пропаганда
любая форма распространения информации в поддержку заданных целей, рассчитанная на влияние на мнения, эмоции, отношения или поведение отдельных индивидов или групп, в том числе социальных.

Пространства информационного субъекты
физические и юридические (общественные организации, хозяйствующие субъекты, органы государственной власти) лица, вступающие для реализации своих потребностей или возложенных на них функций во взаимоотношения с использованием *информации* и *инфраструктур информационных*.

Пространство информационное (инфосфера)
сфера человеческой деятельности, связанная с созданием, преобразованием и использованием информации, включая индивидуальное и общественное сознание, *инфраструктуру информационно-телекоммуникационную* и собственно *информацию*. Образуется совокупностью субъектов информационного взаимодействия или воздействия; собственно информации, предназначенной для использования субъектами, инфраструктуры, обеспечивающей возможность осуществления обмена информацией между субъектами, общественных отношений, складывающихся в связи с формированием, передачей, распространением, хранением и обменом информацией внутри общества.

Противоборство информационное

1) форма межгосударственного противоборства, предусматривающая целенаправленное использование специально разработанных средств для воздействия на *ресурс информационный* противостоящей стороны и защиты собственных ресурсов в интересах достижения поставленных политических и военных целей;

2) форма межгосударственного соперничества, реализуемая посредством оказания *воздействия информационного* на системы управления других государств и их вооруженных сил, а также на политическое и военное руководство и общество в целом, *инфраструктуру информационную* и СМИ этих государств для достижения выгодных себе целей при одновременной защите от аналогичных действий своего *пространства информационного*.

Противоинформация

действия по подавлению *информсферы* противника.

Противоинформация защитная

действия, направленные на защиту своей военной информации от *воздействия информационного* противника.

Противоинформация наступательная

действия, направленные против защитных информационных функций противника.

Противообман

действия, направленные на опровержение, нейтрализацию, принижение влияния или выгоды противника от действия *обмана*. *Противообман* не включает функцию анализа и идентификации действий обмана противника.

Процессы информационные

процессы создания, сбора, анализа, накопления, хранения, поиска, распространения и потребления информации с использованием *инфраструктуры информационной* любого вида или формы. Эти процессы могут быть одиночными или включающими несколько, которые в совокупности составляют более крупную систему или системы процессов.

Прошивка

точно так же, как в программное обеспечение, в постоянные запоминающие устройства (ПЗУ) могут быть заложены компоненты, выполняющие непредусмотренные функции. Производители аппаратного обеспечения, прежде всего устройств с ПЗУ (например, BIOS), могут таким образом внедрять *бомбы логические* или устанавливать *черные ходы* в компьютерных системах. Изменения в программное обеспечение различных ПЗУ могут быть внесены и другими лицами, что, например, уже делалось при перепрограммировании модемов. С широким использованием флэш-BIOS процедура таких изменений значительно упростилась.

Псевдощель

дополнительная (не скрытая) точка входа, преднамеренно внедренная в операционную систему как западня для *соумышленников*.

Разработка социальная

1) термин, используемый в социальной практике для произведения попыток *доступа неправомочного к* компьютеру (информационной системе), своего рода «catch-all» для выявления возможности получить предназначенный доступ или информацию, приближающую этот доступ;

2) нападение, основанное при обмане пользователей или администраторов на целевом участке. Социальные технические нападения типично выполняются, общаясь по телефону с пользователем или оператором и симулируя действия в качестве уполномоченного пользователя, пытаться получать незаконный доступ к системам.

Расплавливание (Ethernet-расплавливание)
форма *атаки,* направленной на перенасыщение Ethernet-узла. Как правило, организуется IP передача, адресованная несуществующему узлу получателя. Это вынуждает маршрутизатор тратить циклы обработки на бесполезный поиск в попытке определить несуществующего получателя и ускорять передачу в ущерб обеспечению нормального движения по сети. Это может являться эффективным средством для *деградации обслуживания* или даже временного *отказа в обслуживании* в данном узле.

Ресурсов информационных владелец
субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом.

Ресурсов информационных собственник
субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами.

Ресурсы информационные
инфраструктура информационная, а также информационные массивы, базы данных и собственно информация и ее потоки, отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других видах информационных систем).

Ретро-вирус
вирус, который не приступает к изменению (разрушению) информации (программ), ожидая, пока все возможные резервные средства восстановления информации не инфицированы настолько, чтобы было невозможно восстановить систему к неинфицированному состоянию.

Рынок информационный
часть общего рынка товаров и услуг. Образуется совокупностью организационных и нормативных механизмоввыявления и удовлетворения потребности физических и юридических лиц в информации по различным аспектам жизнедеятельности человека, общества и государства. В качестве основных элементов *рынка информационного* выступает система организаций, специализирующихся на сборе, обработке и продаже информационных продуктов потребителям.

Сведения критические
сведения, которые требуют непосредственного (немедленного) внимания и реагирования командующего. Включают, но не ограничиваются следующим:
— явные признаки неизбежной вспышки военных действий любого типа (предупреждение нападения);
— агрессия любого характера (природы) против дружественной страны;
— признаки использования ОМУ;
— существенные признаки в пределах потенциальных вражеских стран, которые могут вести к модификации стратегических планов.

Сведения, составляющие государственную тайну
защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести вред безопасности государства.

Связи безопасность
обеспечение защиты, являющееся результатом всех мер, направленных на недопущение лиц, не имеющих на то разрешения, к ценной информации, которая может быть извлечена при обладании и изучении сообщений систем связи, или на введение в заблуждение лиц, не имеющих допуска, в их интерпретировании результатов такого обладания и изучения. Безопасность связи включает в себя обес-

печение безопасности закрытой связи, безопасность радиопередач, обеспечение безопасности работы средств связи и электронного оборудования и обеспечение физической безопасности материалов и информации по вопросам безопасности связи.

Обеспечение безопасности закрытой связи — компонент обеспечения безопасности связи, являющийся результатом наличия технически совершенных криптосистем и их правильного использования.

Безопасность радиопередач — компонент обеспечения безопасности связи, являющийся результатом всех мер, направленных на защиту радиопередач от перехвата и использования в других целях, кроме криптоанализа.

Обеспечение безопасности средств связи и электронного оборудования — компонент обеспечения безопасности связи, являющийся результатом всех мер, предпринимаемых, чтобы не допустить лиц, не имеющих на то разрешения, к ценной информации, которая может быть извлечена из перехвата и анализа излучений шифровального оборудования и систем дальней связи.

Физическая безопасность связи — компонент обеспечения безопасности связи, являющийся результатом всех физических мер, необходимых для защиты секретного оборудования, материалов и документов от доступа к ним или наблюдения за ними со стороны лиц, не имеющих на то разрешение.

Связи сети

совокупность электрических сетей связи и сетей почтовой связи. Они функционируют как взаимоувязанный производственно-хозяйственный комплекс, предназначенный для удовлетворения нужд граждан, органов государственной власти и управления, обороны, безопасности, охраны правопорядка, физических и юридических лиц в услугах электрической и почтовой связи.

Связи электрической сети

сети передачи и приема любых знаков, сигналов, текста, изображений, звуков по проводной, радио-, оптической и другим электромагнитным системам. Системы передачи данных являются разновидностью систем электрической связи, в которых передача информации осуществляется в цифровом виде и на основе специальных протоколов обмена информацией между отправителем и получателем.

Связь почтовая

единая технологическая сеть учреждений и транспортных средств, обеспечивающих прием, обработку, перевозку и доставку почтовых отправлений (письма и почтовые карточки, бандероли, пакеты, посылки, почтовые контейнеры, печатные издания в соответствующей упаковке), перевод денежных средств, а также организацию экспедирования, доставки и распространения периодической печати, денежных выплат целевого назначения.

Секретности информации обеспечение

охрана и защита *информации* и *систем информационных* от несанкционированного доступа или от изменения информации во время ее хранения, обработки или передачи, а также против воспрещения обслуживания имеющих допуск пользователей. Обеспечение секретности информации включает меры, необходимые для обнаружения, документирования и противодействия таким угрозам. Обеспечение секретности информации состоит из *безопасности компьютерной* и *связи безопасности*.

Синие коробки

устройства, созданные *кракерами* и телефонными *хакерами — фрикерами,* чтобы ворваться в телефонную систему и через нее сделать запросы, в обход нормального средства управления и/или процедур контроля доступа.

Система информационная

1) полная инфраструктура, организация, персонал и компоненты, которые участвуют в сборе, обработке (изменении, обновлении), хранении, передаче, демонстрации и распространении информации;

2) организационно упорядоченная совокупность документов и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Спам

метод *кибератаки* — принудительное направление больших количеств, как правило, бессмысленной информации в один или несколько связанных адресов сети. Цель достигается переполнением входных буферов объектов нападения и выведение их из строя, когда они будут вынуждены отказывать в обслуживании другим пользователям. Метод особенно применим к узловым серверам больших сетей. В этом случае из строя выходит фактически целая подсеть.

Спуфинг

обобщенный термин, относящийся к методам *проникновения* в информационные массивы или сети за счет симуляции полномочного пользователя или совершение каких-либо операций в информсетях с неправомерным использованием полномочий или идентифицирующих признаков законного пользователя.

Спуфинг сетевой

получение доступа к ресурсам сети путем обмана, прикрываясь другим адресом: ситуация, когда пользователь пытается соединиться с сервером Интернет, ргоху-сервером или брандмауэром, используя ложный IP-адрес.

Среда информационная

совокупность отдельных лиц, организаций или систем, занимающихся сбором, обработкой и распространением информации; также сюда включается сама информация.

Средства информации психологические

информационные средства (технические или не технические), которые устанавливают любой вид связи с потенциальными клиентами, используя психологические методы или психологические особенности клиента.

Средства информационные

технико-программные и телекоммуникационные средства, используемые в *процессах информационных.*

Средства передачи данных технические

сети связи и устройства, используемые в процессе передачи информации.

Средства психотронные

специальные технические (генераторы излучений), информационные (видеография и телевизионная информация), химические и прочие средства, предназначенные для дистанционного воздействия на население и группы людей с целью вызвать психические и психофизические изменения (краткосрочного или долговременного характера).

Структуры критически важные

1) элементы политико-экономической структуры государства, дестабилизация или блокирование деятельности которых катастрофически скажется на функционировании государства в целом; 2) объекты, системы и институты государства, целенаправленное воздействие на *ресурсы информационные* которых может иметь последствия, прямо затрагивающие национальную безопасность (транспорт, энергоснабжение, кредитно-финансовая сфера, связь, органы государственного управления, система обороны, правоохранительные органы, стратегические информационные ресурсы, научные объекты и научно-технические разработки, объекты повышенной техни-

ческой и экологической опасности, органы ликвидации последствий стихийных бедствий и иных чрезвычайных ситуаций).

Суверенитет интеллектуальный

право субъекта распоряжаться собственным интеллектом, развивать его, реализовывать его возможности, добывать знания и самостоятельно оценивать поступающую информацию не в ущерб другим субъектам.

Сфера информационно-психологическая

часть информационной сферы, связанная с воздействием *информации* на психическую деятельность человека. Она образуется совокупностью людей, *информацией,* которой они обмениваются и которую воспринимают, общественных отношений, возникающих в связи с информационным обменом и информационными воздействиями на психику человека.

Телекоммуникации средства

совокупность средств связи, обеспечивающих передачу данных между ЭВМ и информационными системами, удаленными друг от друга на значительные расстояния.

Терроризм информационный

1) использование информационных средств в террористических целях — угрозы применения или применения физического насилия в политических целях, запугивания и дестабилизации общества и таким образом оказания влияния на население или государство;

2) действия по дезорганизации автоматизированных информационных систем, создающие опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, если они совершены в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти, а также угроза совершения указанных действий в тех же целях.

В узко правовом смысле информационный терроризм может трактоваться как намеренное злоупотребление средствами информационной системы, информационной сети или их компонентом в целях поддержания или способствования террористической деятельности или отдельному такому действию. В этом случае злоупотребление системой (сетью) не обязательно приводит к прямому насилию против людей, но может быть причиной катастроф или диверсий, в результате которых могут быть человеческие жертвы.

Терроризм информационный международный

использование телекоммуникационных и информационных систем и ресурсов и воздействие на них в международном информационном пространстве в террористических целях.

Технология информационная

1) упорядоченная совокупность процессов и действий по созданию *ресурса информационного;*

2) упорядоченная совокупность процессов и действий, в которых для достижения поставленных целей в качестве основных средств и инструментария используются *средства информационные;*

3) организованная совокупность процессов, элементов, устройств и методов, используемых для обработки информации.

Точность информации

термин используется для характеристики того, что информация поддержана и передана таким способом, что не могла измениться ни злонамеренно, ни случайно. Точность гарантирует против подделки или вмешательства. Нередко трактуется как синоним *целостности.*

Троянский конь

1) независимая программа, исполняющая оговоренные в системе функции, но за счет содержащегося в ней сокрытого куска также производит и неправомерные действия в системе в соответствии с заложенным в этот кусок заданием, часто выступая от имени и с правами пользователя и приводя к фальсификации или разрушению данных;

2) фрагмент компьютерного кода, скрытый внутри инфицированной программы. Является широко используемым механизмом маскировки проникновения *вирусов* или *червей* в систему. Могут маскироваться, в частности, под служебные программы, поставляемые с коммерческими и иными программными комплексами обеспечения безопасности компьютерных систем.

Угроза пассивная

угроза неправомочного раскрытия информации без того, чтобы изменять состояние системы. Тип угрозы, которая подразумевает только перехват, но не изменение или уничтожение информации.

Услуг информационных индустрия

сектор экономики, связанный с производством информационных продуктов, т.е. информации, представленной в виде товара.

Услуги информационные

действия субъектов (собственников и владельцев) по обеспечению *пользователей продуктами информационными*.

Уязвимость

в данном контексте: известный или подозреваемый недостаток в аппаратных средствах, программном обеспечении иди функционировании *системы информационной* (сети), который подвергает систему опасности *проникновения,* а циркулирующую в ней информацию случайному раскрытию. Слабость автоматизированных процедур безопасности системы, административных средств управления, физического расположения, внутреннего управления и т.д., которая чревата угрозой получения *злоумышленником* неправомерного доступа к информации или случайным прерыванием процессов обработки с искажением или уничтожением информации.

В *операциях информационных* — слабость в проекте, методиках, выполнении и внутреннем контроле безопасности информационной системы, которые могут быть использованы для получения *доступа несанкционированного* к *информации* или *системе информационной*.

Фаэрвол

метафорическое название типа аппаратных средств ЭВМ и ресурсов системы защиты компонентов программного обеспечения (например, серверов) от *нападения* через сеть (например, от пользователей Интернета) за счет перехвата и проверки поступающей информации сети.

Соединение аппаратных средств ЭВМ и программного обеспечения, выполняющего фаэрвол-действия, может изменяться в зависимости от доминирующих целей защиты и конфигурации защищаемых систем. Система или комбинация систем, которая предписывает границу между двумя или больше сетями. Ворота, которые ограничивают доступ между сетями в соответствии с «местной» политикой безопасности.

Фишбол

тактика обороны от кибератак, в которой неправомочному пользователю разрешают продолжить установленный доступ *к* защищенной системе (сети), но ограничивают взаимодействием только с частью системы (сети) в пределах безопасной области его возможных действий (например, направляют по неправильному адресу на изолированный компьютер; переадресуют к фиктивной окружающей среде, моделирующей фактический сервер) так, чтобы сотрудники службы безо-

пасности могли наблюдать и анализировать намерения атакующего, его тактику, и/или пытаться идентифицировать его. Таким образом, целью этой тактики является содержать, изолировать и контролировать неправомочного пользователя в пределах системы, чтобы получать информацию о нем самом.

Фракер

злоумышленник, комбинирующий хакерские действия и *фрик телефонный.*

Фрик телефонный

вторжение в телефонные системы и системы коммуникаций. Акт использования технологии для нападения на телефонную систему. «Искусство» взламывания телефонной сети. Однако фрик — угроза не только телефонным системам, но и компьютерным сетям и любым системам, использующим телефонные каналы связи.

Фрикер

разновидность *хакера.* Имеет большинство характеристик хакера, по отношению к взлому телефонных систем.

Хакер

обобщенное название *злоумышленника,* намеренно находящего доступ к компьютерам и информационным системам, к которым он не допущен. Хакерские действия не обязательно связаны с нарушением информации, но всегда с незаконным проникновением в закрытые информационные системы и сети.

Целостность (информации)

неизменность и неразделимость информации при ее хранении и передаче внутри системы или сети.

Часовая мина

бомба логическая, программная компонента, активизация которой производится, например, в соответствии с установленной датой и временем. Может рассматриваться как вариант *троянского коня,* в котором заложена активизация по временному условию.

Червь программный

программа или выполнимый модуль, который способен к самостоятельной активной деятельности, воспроизведению и распространению в распределенных системах или сетях. *Червь программный* может копировать себя, если необходимо, чтобы распространиться на все необходимые ему для собственной обработки ресурсы системы. Такими ресурсами могут быть СРЦ времени, каналы ввода-вывода или памяти системы. *Червь программный* будет копировать себя с машины на машину с использованием связей, установленных внутри сети, часто забивая сети и компьютерные системы. Чтобы копировать себя, *червь* должен породить процесс; это подразумевает то, чтобы активно существовать, *черви* требуют мультиуправления задачами.

В отличие от компьютерных вирусов, *червь* представляет собой самостоятельный программный пакет, предназначенный для самораспространения путем копирования своего пакета с одного компьютера на другой, как правило, через сеть, в том числе и Интернет.

Червь сети

червь программный, который мигрирует по сети, копируя себя от одной системы к другой, эксплуатируя общие средства обслуживания сети, заканчиваясь выполнением (копированием) *червя* в новой системе. Позволяет в соответствии со своим предназначением нарушать работоспособность сети или получать доступ к информационным ресурсам сети, подвергшейся *атаке.*

Чехарда (Leapfrog-падение)

1) любая форма вторжения (нападения), выполненного через по крайней мере однудругую промежуточную систему; 2) нелегальное использование идентифицирующих признаков третьего законного пользователя (или итерационно нескольких пользователей) для сокрытия следов проникновения в сеть.

Шторм почтовый
род *атаки*. Целевая акция инспирирования непомерно большого потока почтовых e-mail сообщений, достаточного для полного прерывания нормальных действий машины или сервера адресата.

Экспертная система
система, основанная на знаниях, обеспечивающая решение задач в специальной или прикладной области, получая выводы из базы знаний, созданной на основе опыта человека. Термин «экспертная система» иногда используется в качестве синонима термина «система, основанная на знаниях», но следует сделать акцент на экспертных знаниях. Некоторые *экспертные системы* могут совершенствовать свою базу знаний и развивать новые правила выводов, базирующиеся на их опыте, связанном с предшествующими проблемами.

Электронная торговля
заключение путем обмена электронными документами следующих сделок, предусмотренных ГК РФ (но не ограничиваясь ими): купля-продажа, поставка, возмездное оказание услуг, перевозка, заем и кредит, финансирование под уступку денежного требования, банковский вклад, банковский счет, расчеты, хранение, страхование, поручение, комиссия, агентирование, доверительное управление имуществом, коммерческая концессия, простое товарищество, публичное обещание награды, публичный конкурс, а также приобретение и осуществление с использованием электронных средств иных прав и обязанностей в сфере предпринимательской деятельности. Торговля, осуществляемая с помощью электронного документооборота в Интернете.

Электронная цифровая подпись (ЭЦП)
набор символов, вырабатываемый средствами электронной цифровой подписи и являющийся неотъемлемой частью электронного документа. Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. Аналог собственноручной подписи физического лица, представленный как последовательность символов, полученной в результате криптографического преобразования электронных данных с использованием закрытого ключа ЭЦП, позволяющая пользователю открытого ключа установить целостность и неизменность этой информации, а также владельца закрытого ключа ЭЦП.

Электронная экономика
в широком смысле: экономика, основанная на широком использовании информации, знаний и информационно-коммуникационных технологий (ИКТ). В узком смысле: экономика, базирующаяся на сетевых технологиях и моделях «бизнес — бизнес» (B2B) и «бизнес — потребитель» (B2C).

Электронный архив
архив документов, представленных в электронной форме, пригодной для использования в автоматизированных информационных системах.

Электронный бизнес
e-Business, электронная коммерция, интернет-бизнес — синонимы. Понятие более широкое, чем электронная торговля, включающее наличие своего сайта в Интернете, виртуального магазина, системы управления компанией, использование электронной рекламы, маркетинга, модели «бизнес для бизнеса» (B2B) или «бизнес для потребителя» (B2C).

Список принятых сокращений

АИС
Автоматизированная информационная система
ВВУИО
Всемирная встреча на высшем уровне по вопросам глобального информационного общества
ГИО
Глобальное информационное общество
ГРН
Государственный регистр населения
ДЦТ
Доступ к цифровым технологиям
ИАС
Информационно-аналитические средства
ИКР
Интеллектуальный кабинет руководителя
ИКТ
Информационно-коммуникационные технологии
ИТКС
Информационно-телекоммуникационная сеть
КТС
Комплекс технических средств
КЦ
Кризисный центр
ЛВС
Локальная вычислительная сеть
МИБ
Международная информационная безопасность
МСУ
Местное самоуправление
ЭП
Электронное правительство
ОИТКС
Открытые информационно-телекоммуникационные сети
СПУН
Система персонального учета населения
СЦ
Ситуационный центр
ТНК
Транснациональная корпорация
ГПЭ
Группа правительственных экспертов
ФЦП
Федеральная целевая программа
ЭДО
Электронный документооборот
ЭЦП
Электронная цифровая подпись

ПРИЛОЖЕНИЯ

Генеральная Ассамблея

Distr.: General
16 December 2004

Пятьдесят девятая сессия
Пункт 60 повестки дня

Резолюция, принятая Генеральной Ассамблеей

[по докладу Первого комитета (A/59/454)]

59/61. 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 и 58/32 от 8 декабря 2003 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,

учитывая итоги Совещания на уровне министров по проблеме терроризма, которое состоялось в Париже 30 июля 1996 года, а также принятые на нем рекомендации[1],

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 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 и 58/32,

принимая к сведению доклады Генерального секретаря, содержащие эти оценки[2],

отмечая с удовлетворением инициативу Секретариата и Института Организации Объединенных Наций по исследованию проблем разоружения по проведению в Женеве в августе 1999 года международной встречи экспертов по вопросу о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также ее результаты,

считая, что оценки государств-членов, содержащиеся в докладах Генерального секретаря, а также международная встреча экспертов способствовали лучшему пониманию существа проблем международной информационной безопасности и связанных с ними понятий,

1. *призывает* государства-члены и далее содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также возможных мер по ограничению угроз, возникающих в этой сфере, исходя из необходимости сохранить свободный поток информации;

2. *полагает*, что целям таких мер соответствовало бы изучение соответствующих международных концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем;

3. *просит* все государства-члены продолжать информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:

a) общая оценка проблем информационной безопасности;

b) определение основных понятий, относящихся к информационной безопаснос-

[1] См. A/51/261, приложение.

[2] 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 и A/59/116 и Add.1.

ти, включая несанкционированное вмешательство или противоправное использование информационных и телекоммуникационных систем и информационных ресурсов;

c) содержание концепций, упомянутых в пункте 2 выше;

4. *с удовлетворением отмечает*, что Генеральный секретарь рассматривает существующие и потенциальные угрозы в сфере информационной безопасности и возможные совместные меры по их устранению, а также проводит исследование концепций, упомянутых в пункте 2 выше, с помощью созданной в 2004 году в соответствии с резолюцией 58/32 группы правительственных экспертов и представит доклад орезультатах данного исследования Генеральной Ассамблее на ее шестидесятой сессии;

5. *с удовлетворением отмечает также*, что группа правительственных экспертов, учрежденная Генеральным секретарем, провела свою первую сессию 12.16 июля 2004 года в Нью-Йорке и что она намерена провести еще две сессии в 2005 году для выполнения своего мандата, определенного резолюцией 58/32;

6. *постановляет* включить в предварительную повестку дня своей шестидесятой сессии пункт, озаглавленный «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

66-е пленарное заседание,
3 декабря 2004 года

Всемирная встреча на высшем уровне по вопросам **информационного общества**
Женева, 2003 г. – Тунис, 2005 г.

Документ WSIS-03/GENEVA/DOC/4-R
12 декабря 2003 года
Оригинал: английский

Декларация принципов

Построение информационного общества — глобальная задача в новом тысячелетии

A. Наша общая концепция информационного общества

1. **Мы, представители народов мира, собравшиеся в Женеве 10–12 декабря 2003 года для проведения первого этапа Всемирной встречи на высшем уровне по вопросам информационного общества**, заявляем о нашем общем стремлении и решимости построить ориентированное на интересы людей, открытое для всех и направленное на развитие информационное общество, в котором каждый мог бы создавать информацию и знания, иметь к ним доступ, пользоваться и обмениваться ими, с тем чтобы дать отдельным лицам, общинам и народам возможность в полной мере реализовать свой потенциал, содействуя своему устойчивому развитию и повышая качество своей жизни на основе целей и принципов Устава Организации Объединенных Наций и соблюдая в полном объеме и поддерживая Всеобщую декларацию прав человека.

2. **Наша задача** состоит в том, чтобы использовать потенциал информационных и коммуникационных технологий для достижения сформулированных в Декларации тысячелетия целей развития, а именно ликвидации крайней нищеты и голода, обеспечения всеобщего начального образования, содействия равенству мужчин и женщин и расширению прав и возможностей женщин, сокращения детской смертности, улучшения охраны материнства, борьбы с ВИЧ/СПИДом, малярией и другими заболеваниями, содействия экологической устойчивости и формирования глобального партнерства в целях развития для обеспечения более мирного, справедливого и процветающего мира. Мы также подтверждаем свою приверженность достижению устойчивого развития и согласованных целей развития, изложенных в йоханнесбургских Декларации и Плане выполнения решений и Монтеррейском консенсусе, а также в других документах соответствующих встреч на высшем уровне в рамках Организации Объединенных Наций.

3. **Мы вновь подтверждаем** универсальность, неделимость, взаимозависимость и взаимосвязь всех прав человека и основных свобод, включая право на развитие, как это закреплено в Венской декларации. Мы вновь подтверждаем также, что демократия, устойчивое развитие и соблюдение прав человека и основных свобод, а также надлежащее государственное управление на всех уровнях являются взаимозависимыми и взаимоукрепляющими. Мы далее решаем укреплять уважение верховенства права в области внешней и внутренней политики.

4. **Мы вновь подтверждаем**, что мы признаем в качестве необходимого фундамента информационного общества провозглашенное в статье 19 Всеобщей декларации прав человека право каждого человека на свободу убеждений и на свободное их выраже-

ние; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ. Общение является одним из основополагающих социальных процессов, одной из базовых человеческих потребностей и фундаментом любой социальной организации. Оно составляет сердцевину информационного общества. Каждый, где бы он ни находился, должен иметь возможность участвовать в информационном обществе, и никого нельзя лишить предлагаемых этим обществом преимуществ.

5. **Мы вновь подтверждаем далее** свою приверженность положениям статьи 29 Всеобщей декларации прав человека, согласно которым каждый человек имеет обязанности перед обществом, в котором только и возможно свободное и полное развитие его личности, и при осуществлении своих прав и свобод каждый человек должен подвергаться только таким ограничениям, какие установлены законом исключительно с целью обеспечения должного признания и уважения прав и свобод других и удовлетворения справедливых требований морали, общественного порядка и общего благосостояния в демократическом обществе. Осуществление таких прав и свобод ни в коем случае не должно вступать в противоречие с целями и принципами Организации Объединенных Наций. Тем самым мы будем содействовать созданию информационного общества, в котором уважается достоинство человеческой личности.

6. В соответствии с духом настоящей Декларации **мы вновь заявляем о своей решимости** соблюдать принцип суверенного равенства всех государств.

7. **Мы сознаем, что наука** играет центральную роль в развитии информационного общества. Многие компоненты информационного общества являются результатом научно-технических достижений, ставших возможными благодаря совместному использованию результатов исследований.

8. **Мы сознаем**, что образование, знания, информация и общение составляют основу развития, инициативности и благополучия человеческой личности. Наряду с этим информационные и коммуникационные технологии (ИКТ) оказывают огромное влияние практически на все аспекты нашей жизни. Стремительный прогресс этих технологий открывает совершенно новые перспективы достижения более высоких уровней развития. Способность этих технологий ослабить воздействие многих традиционных препятствий, в особенности связанных с временем и расстоянием, впервые в истории дает возможность использовать потенциал этих технологий во благо миллионов людей во всех уголках земного шара.

9. **Мы осознаем,** что ИКТ следует рассматривать как инструмент, а не как самоцель. При благоприятных условиях эти технологии способны стать мощным инструментом повышения производительности, экономического роста, создания новых рабочих мест и расширения возможностей трудоустройства, а также повышения качества жизни для всех. Они также могут содействовать ведению диалога между народами, странами и цивилизациями.

10. **Мы также в полной мере осознаем,** что сегодня преимущества революции в области информационных технологий неравномерно распределены между развитыми и развивающимися странами, а также внутри стран. Мы полны решимости превратить этот разрыв в цифровых технологиях в цифровые возможности для всех, прежде всего для тех, кому грозят отставание и дальнейшая маргинализация.

11. **Мы привержены** идее претворения в жизнь нашей общей концепции информационного общества на благо нынешнего и будущих поколений. Мы сознаем, что молодежь представляет собой будущий трудовой ресурс, играет ведущую роль в создании ИКТ и быстрее других осваивает эти технологии. Поэтому следует предоставить ей возможность учиться, творить, вносить свой вклад, заниматься предпринимательской деятельностью и участвовать в принятии решений. Особое внимание мы

должны уделять тем молодым людям, которые пока не имеют возможности в полной мере пользоваться преимуществами, предоставляемыми ИКТ. Мы также признаем необходимым обеспечить соблюдение прав ребенка, равно как и защиту детей и их благополучие при разработке приложений и предоставлении услуг на базе ИКТ.

12. **Мы подтверждаем**, что развитие ИКТ открывает грандиозные перспективы для женщин, которые должны составлять неотъемлемую часть информационного общества и стать его ключевыми участниками. Мы признаем необходимым обеспечить, чтобы в информационном обществе женщинам предоставлялись все права и возможности и чтобы они в полной мере участвовали на равных основаниях во всех сферах жизни общества и во всех процессах принятия решений. Для этого мы должны включить в основные направления нашей деятельности принцип равноправия женщин и мужчин и применять ИКТ как инструмент для достижения этой цели.

13. При построении информационного общества **мы должны уделять первоочередное внимание** особым потребностям маргинализированных и уязвимых групп общества, в том числе мигрантов, внутренне перемещенных лиц и беженцев, безработных и обездоленных людей, меньшинств и кочевых народов. Мы должны также учитывать особые потребности престарелых и лиц с ограниченными возможностями.

14. **Мы преисполнены решимости** расширить возможности неимущих, прежде всего проживающих в отдаленных, сельских и маргинализированных городских районах, в отношении доступа к информации и использования ИКТ как инструмента, помогающего им в их усилиях избавиться от нищеты.

15. При становлении информационного общества первоочередное внимание следует уделять особому положению коренных народов, а также сохранению их наследия и культурного достояния.

16. **Мы продолжаем уделять** особое внимание специфическим потребностям жителей развивающихся стран, стран с переходной экономикой, наименее развитых стран, малых островных развивающихся государств, развивающихся стран, не имеющих выхода к морю, бедных стран с крупной задолженностью, оккупированных стран и территорий, стран, преодолевающих последствия конфликтов, а также стран и регионов с особыми потребностями, равно как и представляющим серьезную угрозу для развития обстоятельствам, в том числе стихийным бедствиям.

17. **Мы сознаем**, что для создания открытого для всех информационного общества требуются новые формы солидарности, партнерства и сотрудничества между органами государственного управления и другими заинтересованными сторонами, то есть частным сектором, гражданским обществом и международными организациями. Осознавая, что поставленная в настоящей Декларации масштабная задача — преодоление разрыва в цифровых технологиях и обеспечение гармоничного, справедливого и равноправного развития для всех — потребует твердой решимости всех заинтересованных сторон, мы призываем к цифровой солидарности как на национальном, так и на международном уровне.

18. Ничто в настоящей Декларации не должно истолковываться как посягательство на положения Устава Организации Объединенных Наций, Всеобщей декларации прав человека, любых других международных документов или национального законодательства, принятых в поддержку этих документов, как противоречие им, их ограничение или отступление от них.

B. Информационное общество для всех: основные принципы

19. **Мы преисполнены решимости,** строя информационное общество, обеспечить, чтобы каждый мог воспользоваться возможностями, которые могут предоставить ИКТ. Мы согласны в том, что для решения этих задач все заинтересованные стороны должны работать сообща над расширением доступа к информационным и коммуникационным инфраструктурам и технологиям, а также к информации и знаниям, наращи-

вать потенциал, повышать доверие и безопасность при использовании ИКТ, создавать на всех уровнях благоприятную среду, разрабатывать приложения ИКТ и расширять сферу их применения, содействовать культурному разнообразию и уважать его, признавать роль средств массовой информации, уделять внимание этическим аспектам информационного общества и поощрять международное и региональное сотрудничество. Мы согласны в том, что это — ќлючевые принципы построения открытого для всех информационного общества.

1) Роль органов государственного управления и всех заинтересованных сторон в содействии применению ИКТ в целях развития

20. Органам государственного управления, а также частному сектору, гражданскому обществу, Организации Объединенных Наций и другим международным организациям надлежит сыграть важную роль в развитии информационного общества, взять на себя за это ответственность и в надлежащих случаях участвовать в процессах принятия решений. Построение информационного общества, ориентированного на интересы людей, является общим делом, требующим сотрудничества и партнерских отношений между всеми заинтересованными сторонами.

2) Информационная и коммуникационная инфраструктура — необходимый фундамент открытого для всех информационного общества

21. Обеспечение подключения является одним из главных факторов построения информационного общества. Предоставление универсального, повсеместного, справедливого и приемлемого в ценовом отношении доступа к инфраструктуре ИКТ и услугам на базе ИКТ составляет одну из задач информационного общества и должно стать целью всех заинтересованных сторон, участвующих в его построении. Обеспечение подключения также предусматривает доступ к услугам энергоснабжения и почтовой связи, который следует обеспечивать в соответствии с национальным законодательством каждой страны.

22. Хорошо развитая инфраструктура информационных и коммуникационных сетей и приложения, отвечающие региональным, национальным и местным условиям, легкодоступные и приемлемые в ценовом отношении, позволяющие в большей степени использовать широкополосную связь и другие инновационные технологии там, где это возможно, способны ускорить социально-экономический прогресс стран и повысить благосостояние всех людей, общин и народов.

23. Политика, создающая на всех уровнях благоприятные условия для стабильности, предсказуемости и добросовестной конкуренции, должна разрабатываться и осуществляться так, чтобы не только в больших масштабах привлекать частные инвестиции в развитие инфраструктуры ИКТ, но и обеспечивать выполнение обязательств по универсальному обслуживанию в тех областях, где не действуют традиционные рыночные механизмы. В находящихся в неблагоприятных условиях районах создание публичных пунктов доступа к ИКТ в таких структурах, как почтовые отделения, школы, библиотеки и архивы, может служить эффективным способом обеспечения универсального доступа к инфраструктуре и услугам информационного общества.

3) Доступ к информации и знаниям

24. Обеспечение каждому возможности иметь доступ к информации, идеям и знаниям и вносить в эти области свой вклад является необходимым элементом открытого для всех информационного общества.

25. Совместному использованию и расширению глобальных знаний в целях развития может способствовать устранение барьеров на пути достижения равноправного доступа к информации для осуществления деятельности в области экономики, в социальной сфере, политике, здравоохранении, культуре, образовании и науке, а также упрощение доступа к информации, являющейся публичным достоянием, в том числе путем обеспечения универсального дизайна и использования ассистивных технологий.

26. Наличие обширного публичного достояния – важнейшая составляющая развития информационного общества, обеспечивающая такие многочисленные преимущества, как получение населением образования, создание новых рабочих мест, инновационная деятельность, открытие перспектив в хозяйственной сфере и научный прогресс. Информация, относящаяся к публичному достоянию, должна быть легкодоступной в интересах развития информационного общества и должна быть защищена от незаконного присвоения. Следует укреплять публичные учреждения, такие как библиотеки и архивы, музеи, собрания культурных ценностей и другие коллективные пункты доступа, с тем чтобы содействовать сохранению документальных записей и свободному и равноправному доступу к информации.

27. Доступу к информации и знаниям можно способствовать путем повышения осведомленности всех заинтересованных сторон о возможностях, предоставляемых различными моделями программного обеспечения, в том числе разрабатываемого отдельными компаниями, программного обеспечения с открытыми кодами и свободно распространяемого программного обеспечения, с тем чтобы усиливать конкуренцию, расширять доступ к ним пользователей и диапазон их выбора, а также дать всем пользователям возможность решать, какой вариант наилучшим образом удовлетворяет их потребностям. Приемлемый в ценовом отношении доступ к программному обеспечению является важным компонентом действительно открытого для всех информационного общества.

28. Мы стремимся содействовать обеспечению всеобщего и равноправного универсального доступа к научным знаниям и созданию и распространению научно-технической информации, включая инициативы по организации свободного доступа к научным публикациям.

4) Наращивание потенциала

29. Каждый человек должен иметь возможность овладевать навыками и знаниями, необходимыми для понимания сути информационного общества и базирующейся на знаниях экономики, активного участия в них и полномасштабного использования их преимуществ. Грамотность и всеобщее начальное образование являются ключевыми факторами при построении открытого для всех без исключения информационного общества, при этом первоочередное внимание должно уделяться особым потребностям девочек и женщин. С учетом потребности на всех уровнях в большом числе специалистов в области ИКТ и информатики особого внимания заслуживает наращивание институционального потенциала.

30. Необходимо содействовать применению ИКТ на всех уровнях образования, профессиональной подготовки и развития людских ресурсов с учетом особых потребностей лиц с ограниченными возможностями, а также находящихся в неблагоприятных условиях и уязвимых слоев населения.

31. Непрерывное образование и образование для взрослых, переподготовка, обучение в течение всей жизни, дистанционное обучение и другие специальные услуги, такие как телемедицина, могут внести решающий вклад в расширение возможностей трудоустройства и содействовать людям в использовании новых перспектив, открываемых ИКТ в отношении традиционных рабочих мест, самозанятости и освоения новых профессий. Необходимым фундаментом для этого являются информированность и грамотность в области ИКТ.

32. Активную роль в формировании информационного общества должны играть разработчики, издатели и производители контента, а также преподаватели, инструкторы, работники архивов и библиотек и учащиеся, в особенности в наименее развитых странах.

33. Для обеспечения устойчивого развития информационного общества следует наращивать национальный потенциал в области научно-технических и опытно-конструкторских работ в сфере ИКТ. Наряду с этим партнерские отношения, в первую очередь между развитыми и развивающимися странами и внутри этих групп стран,

включая страны с переходной экономикой, в области научно-технических и опытно-конструкторских работ, передачи технологий, производства и использования продуктов и услуг на базе ИКТ, являются важнейшим условием содействия наращиванию потенциала и всеобщему участию в информационном обществе. Производство продукции ИКТ открывает широкие перспективы для создания материальных благ.

34. Реализация наших общих стремлений, прежде всего к тому, чтобы развивающиеся страны и страны с переходной экономикой стали полноправными членами информационного общества, и позитивный процесс их интеграции в экономику, базирующуюся на знаниях, во многом зависят от ускорения наращивания потенциала в области образования, технологий, ноу-хау и доступа к информации. Эти факторы являются решающими в определении уровня развития и конкурентоспособности.

5) Укрепление доверия и безопасности при использовании ИКТ

35. Упрочение основы для доверия, включая информационную безопасность и безопасность сетей, аутентификацию, защиту неприкосновенности частной жизни и прав потребителей, является предпосылкой становления информационного общества и роста доверия со стороны пользователей ИКТ. Необходимо формировать, развивать и внедрять глобальную культуру кибербезопасности в сотрудничестве со всеми заинтересованными сторонами и компетентными международными организациями. Данные усилия должны опираться на расширяющееся международное сотрудничество. В рамках этой глобальной культуры кибербезопасности важно повышать безопасность и обеспечивать защиту данных и неприкосновенность частной жизни, расширяя при этом доступ и масштаб торговых операций. Кроме того, необходимо принимать во внимание уровень социально-экономического развития каждой страны и учитывать связанные с ориентацией на развитие аспекты информационного общества.

36. Признавая принципы универсального и недискриминационного доступа к ИКТ для всех стран, мы поддерживаем деятельность Организации Объединенных Наций, направленную на предотвращение возможности использования ИКТ в целях, которые несовместимы с задачами обеспечения международной стабильности и безопасности и способны оказать отрицательное воздействие на целостность государственных инфраструктур, нанося ущерб их безопасности. Следует предотвращать использование информационных ресурсов и технологий в преступных и террористических целях, соблюдая при этом права человека.

37. Спам представляет для пользователей, сетей и в целом для Интернет серьезную проблему, масштабы которой возрастают. Вопросы, касающиеся спама и кибербезопасности, следует рассматривать на соответствующем национальном и международном уровнях.

6) Благоприятная среда

38. Необходимым условием существования информационного общества является благоприятная среда на национальном и международном уровнях. ИКТ следует применять как важный инструмент надлежащего государственного управления.

39. Верховенство права, наряду с благоприятной, прозрачной, способствующей конкуренции, основанной на принципе технологической нейтральности и предсказуемой политической и регламентарной базой, учитывающей национальные особенности, необходимо для создания ориентированного на интересы людей информационного общества. Органы государственного управления должны принимать в надлежащих случаях меры для компенсации неэффективности рыночных механизмов, поддержания добросовестной конкуренции, привлечения инвестиций, содействия развитию инфраструктуры ИКТ и приложений на базе ИКТ, использования в максимальной степени экономических и социальных выгод и учета национальных приоритетов.

40. Жизненно важными дополнительными компонентами относящихся к ИКТ национальных усилий в области развития являются динамичная и благоприятная международная среда, способствующая привлечению прямых иностранных инвестиций, передаче технологий и международному сотрудничеству, в первую очередь в областях финансов, задолженности и торговли, а также полномасштабное и эффективное участие развивающихся стран в принятии решений на мировом уровне. Расширение приемлемой в ценовом отношении возможности глобального подключения может значительно способствовать эффективности этих усилий в области развития.

41. ИКТ, способствуя повышению эффективности и производительности, прежде всего предприятий малого и среднего бизнеса (МСП), являются мощным катализатором экономического роста. В этом отношении развитие информационного общества важно для экономического роста на широкой основе как в развитых, так и в развивающихся странах. Следует поощрять обусловливаемый ИКТ рост производительности и внедрение инноваций в секторы экономики. Справедливое распределение создаваемых благ способствует ликвидации нищеты и социальному развитию. Наиболее благоприятное воздействие будут, вероятно, оказывать те политические стратегии, которые способствуют продуктивным инвестициям и дают возможность предприятиям, в первую очередь МСП, осуществлять перемены, необходимые для извлечения выгоды из применения ИКТ.

42. Для поощрения инновационной деятельности и творчества в информационном обществе важно обеспечивать защиту интеллектуальной собственности; аналогичным образом, широкое распространение, популяризация и совместное использование информации также важны для поощрения инновационной деятельности и творчества. Содействие осознанному участию всех в решении вопросов интеллектуальной собственности и совместном использовании знаний посредством полномасштабного информирования и наращивания потенциала является одним из основополагающих элементов открытого для всех информационного общества.

43. В информационном обществе устойчивому развитию может в наибольшей степени способствовать полномасштабная интеграция относящихся к ИКТ мероприятий и программ в национальные и региональные стратегии развития. Мы приветствуем Новое партнерство в интересах развития Африки (НЕПАД) и призываем международное сообщество поддержать принимаемые в рамках этой инициативы меры, касающиеся ИКТ, а также аналогичные мероприятия, которые осуществляются в других регионах. Распределение выгод от экономического роста, получаемых благодаря применению ИКТ, способствует ликвидации нищеты и обеспечению устойчивого развития.

44. К важнейшим составляющим построения информационного общества относится стандартизация. Особое внимание следует уделять разработке и принятию международных стандартов. Разработка и использование открытых, обеспечивающих возможность взаимодействия, недискриминационных и определяемых спросом стандартов с учетом потребностей пользователей и потребителей, — одно из основных условий развития и расширения распространения ИКТ и обеспечения более приемлемого в ценовом отношении доступа к ним, прежде всего в развивающихся странах. Международные стандарты имеют целью создание среды, в которой потребители могли бы пользоваться соответствующими услугами в любой точке мира, независимо от применяемой технологии.

45. Управление использованием радиочастотного спектра должно осуществляться в интересах общества, в соответствии с принципом законности, при неукоснительном соблюдении национальных законов и норм, а также соответствующих международных соглашений.

46. Государства настоятельно призываются принимать при построении информационного общества меры, направленные на недопущение и отказ от каких-либо односто-

ронних действий, не соответствующих международному праву и Уставу Организации Объединенных Наций и препятствующих полномасштабному обеспечению социально-экономического развития затрагиваемых стран и благосостояния их населения.

47. Поскольку ИКТ постепенно изменяют наши методы работы, основополагающее значение имеет создание защищенных, безопасных и не наносящих ущерба здоровью условий труда, предусматривающих использование ИКТ, при соблюдении всех соответствующих международных норм.

48. Интернет превратился в публичный ресурс глобального масштаба, и управление его использованием должно стать одним из основных вопросов повестки дня информационного общества. Управление использованием Интернет на международном уровне необходимо осуществлять на многосторонней, прозрачной и демократической основе при полномасштабном участии органов государственного управления, частного сектора, гражданского общества и международных организаций. Это управление должно обеспечивать справедливое распределение ресурсов, способствовать доступу для всех, гарантировать стабильное и защищенное функционирование Интернет с учетом многоязычия.

49. Управление использованием Интернет охватывает как технические вопросы, так и вопросы государственной политики, и в нем должны участвовать все заинтересованные стороны и соответствующие межправительственные и международные организации. В связи с этим признается, что:

a) политические полномочия по связанным с Интернет вопросам государственной политики являются суверенным правом государств. Государства имеют права и обязанности в отношении связанных с Интернет вопросов государственной политики международного уровня;

b) частный сектор играет и должен продолжать играть важную роль в развитии Интернет, как в технической, так и в экономической сфере;

c) гражданское общество также играет важную роль в относящихся к Интернет вопросах, в особенности на уровне общин, и должно продолжать играть такую роль;

d) межправительственные организации играют и должны продолжать играть роль, способствующую координации связанных с Интернет вопросов государственной политики;

e) международные организации также играют и должны продолжать играть важную роль в разработке относящихся к Интернет технических стандартов и соответствующей политики.

50. Вопросы управления использованием Интернет на международном уровне следует решать согласованным образом. Мы обращаемся к Генеральному секретарю Организации Объединенных Наций с просьбой учредить рабочую группу по управлению использованием Интернет в рамках открытого и всеобъемлющего процесса, обеспечивающего механизм для полномасштабного и активного участия органов государственного управления, частного сектора и гражданского общества как из развивающихся, так и из развитых стран, в том числе соответствующих межправительственных и международных организаций и форумов, в целях изучения вопроса об управлении использованием Интернет и представления к 2005 году в надлежащих случаях предложений для принятия решения в отношении организации управления использованием Интернет.

7) Приложения на базе ИКТ: преимущества во всех аспектах жизни

51. Использование и развертывание ИКТ должны быть направлены на создание преимуществ во всех аспектах нашей повседневной жизни. Приложения на базе ИКТ потенциально важны для деятельности органов государственного управления и предоставляемых ими услуг здравоохранения и информации об охране здоровья, образования и профессиональной подготовки, занятости, создания рабочих мест, предпринимательства, сельского хозяйства, транспорта, охраны окружающей среды и

рационального использования природных ресурсов, предотвращения катастроф, для развития культуры, а также для ликвидации нищеты и достижения иных согласованных целей в области развития. Кроме того, ИКТ должны способствовать устойчивости структур производства и потребления и преодолению традиционных барьеров, давая тем самым возможность всем получить доступ на местные и глобальные рынки на более равноправной основе. Приложения ИКТ должны быть удобными для пользователей, доступными для всех, приемлемыми в ценовом отношении, соответствовать местным потребностям благодаря адаптации к местным языкам и культуре и поддерживать устойчивое развитие. Для этого местные органы власти должны играть важную роль в предоставлении услуг на базе ИКТ во благо своих граждан.

8) Культурное разнообразие и культурная самобытность, языковое разнообразие и местный контент

52. Культурное разнообразие – это общее наследие человечества. Информационное общество должно основываться на уважении культурной самобытности, разнообразия культур и языков, традиций и религий, стимулировать это уважение и содействовать диалогу между культурами и цивилизациями. Популяризация, укрепление и сохранение различных культур и языков, что отражено в соответствующих документах, принятых Организацией Объединенных Наций, в том числе во Всеобщей декларации ЮНЕСКО о культурном разнообразии, будут далее обогащать информационное общество.

53. При построении открытого для всех информационного общества приоритет следует отдавать созданию, распространению и сохранению контента на разных языках и в различных форматах, при этом особое внимание необходимо уделять разнообразию предложения творческих произведений и должному признанию прав авторов и деятелей искусств. Необходимо содействовать производству и обеспечению доступности всего контента — образовательного, научного, культурного и развлекательного — на разных языках и в различных форматах. Развитие местного контента, отвечающего национальным или региональным потребностям, будет способствовать социально-экономическому развитию и стимулировать участие всех заинтересованных сторон, включая жителей сельских, отдаленных и маргинальных районов.

54. Сохранение культурного наследия представляет собой один из важнейших элементов самобытности и самосознания людей и связывает общество с его прошлым. Информационное общество должно всеми соответствующими методами, включая перевод в цифровую форму, собирать и сохранять культурное наследие для будущих поколений.

9) Средства массовой информации

55. Мы вновь подтверждаем нашу приверженность принципам свободы печати и свободы информации, а также независимости, плюрализма и разнообразия средств массовой информации, которые являются основной составляющей информационного общества. Свобода искать, получать, передавать и использовать информацию для создания, накопления и распространения знаний имеет существенное значение для информационного общества. Мы призываем средства массовой информации ответственно использовать информацию и обращаться с ней, в соответствии с высочайшими этическими и профессиональными стандартами. Традиционные средства массовой информации во всех их видах играют важную роль в информационном обществе, и ИКТ должны способствовать этому. Следует поощрять развитие разнообразных форм собственности на средства массовой информации, в соответствии с национальным законодательством, учитывая при этом соответствующие международные конвенции. Мы вновь подтверждаем необходимость сокращения диспропорций в средствах массовой информации на международном уровне, особенно в том, что касается инфраструктуры, технических ресурсов и развития навыков и умений.

10) Этические аспекты информационного общества

56. В информационном обществе необходимо уважать мир и отстаивать основные ценности, такие как свобода, равенство, солидарность, терпимость, коллективная ответственность и бережное отношение к природе.

57. Мы признаем важность для информационного общества этических норм, которые должны способствовать справедливости, а также поддерживать достоинство и ценность человеческой личности. Максимально надежную защиту следует обеспечить семье, с тем чтобы дать ей возможность играть в обществе решающую роль.

58. При использовании ИКТ и при создании контента следует уважать права человека и основные свободы других людей, включая неприкосновенность частной жизни и право на свободу мысли, совести и религии, согласно положениям соответствующих международных документов.

59. Все участники информационного общества должны предпринимать соответствующие действия и принимать установленные законодательством меры по предотвращению ненадлежащего использования ИКТ, такого как противоправные деяния и прочие действия на почве расизма, расовой дискриминации, ксенофобии и связанные с ними проявления нетерпимости, ненависти, насилия, все формы жестокого обращения с детьми, включая педофилию и детскую порнографию, а также торговля людьми и их эксплуатация.

11) Международное и региональное сотрудничество

60. Мы намереваемся в полной мере использовать предоставляемые ИКТ возможности в нашем стремлении достичь согласованных на международном уровне целей в области развития, в том числе содержащихся в Декларации тысячелетия, а также отстаивать ключевые принципы, изложенные в этой Декларации. Информационное общество глобально по своей сути, и предпринимаемые на национальном уровне усилия необходимо поддерживать посредством эффективного международного и регионального сотрудничества между органами государственного управления, частным сектором, гражданским обществом и другими заинтересованными сторонами, включая международные финансовые учреждения.

61. Для построения открытого для всех глобального информационного общества мы будем изыскивать и эффективно применять на международном уровне конкретные подходы и механизмы, в том числе оказывать финансовую и техническую помощь. Поэтому, оценивая по достоинству сотрудничество в области ИКТ, которое осуществляется в рамках различных механизмов, мы призываем все заинтересованные стороны обязаться принять «Повестку дня цифровой солидарности», содержащуюся в Плане действий. Мы убеждены в том, что согласованная на мировом уровне цель заключается в содействии преодолению разрыва в цифровых технологиях, расширении доступа к ИКТ, создании цифровых возможностей и использовании заключенного в ИКТ потенциала в интересах развития. Мы признаем желание некоторых заинтересованных сторон создать международный добровольный «Фонд цифровой солидарности» и желание других сторон провести исследования, касающиеся существующих механизмов, а также эффективности и целесообразности создания такого фонда.

62. Региональная интеграция способствует развитию глобального информационного общества и делает необходимым тесное сотрудничество в рамках регионов и между ними. Региональный диалог должен содействовать наращиванию потенциала на национальном уровне и приведению национальных стратегий в соответствие с целями настоящей Декларации принципов с учетом национальных и региональных особенностей. В связи с этим мы призываем международное сообщество поддержать принимаемые в рамках таких инициатив меры, касающиеся ИКТ.

63. Мы принимаем решение оказывать содействие развивающимся странам, НРС и странам с переходной экономикой посредством мобилизации средств из

всех источников финансирования, предоставления финансовой и технической помощи и путем создания среды, способствующей передаче технологий, в соответствии с целями настоящей Декларации и Плана действий.

64. Основные сферы компетенции Международного союза электросвязи (МСЭ) в областях ИКТ — содействие в преодолении разрыва в цифровых технологиях, международное и региональное сотрудничество, управление использованием радиочастотного спектра, разработка стандартов и распространение информации — имеют решающее значение для построения информационного общества.

С. К информационному обществу для всех, основанному на совместном использовании знаний

65. **Мы берем на себя обязательство** укреплять сотрудничество, с тем чтобы сообща находить решения проблем и выполнять План действий, претворяя в жизнь концепцию открытого для всех информационного общества, основанного на ключевых принципах, содержащихся в настоящей Декларации.

66. **Мы берем на себя, далее, обязательство** оценивать в количественном отношении процесс преодоления разрыва в цифровых технологиях и осуществлять наблюдение за этим процессом, учитывая различия в уровнях развития, с тем чтобы достичь согласованных на международном уровне целей в области развития, в том числе содержащихся в Декларации тысячелетия, и определять эффективность инвестиций и усилий в сфере международного сотрудничества для построения информационного общества.

67. **Мы твердо убеждены,** что все вместе мы вступаем в новую эру огромных возможностей — эру информационного общества и расширения сферы человеческого общения. В этом зарождающемся обществе информацию и знания можно производить, обмениваться ими, совместно их использовать и передавать по всем сетям мира. Если мы предпримем необходимые действия, вскоре все люди смогут сообща построить новое информационное общество, основанное на совместном использовании знаний, на базе глобальной солидарности и более полного взаимопонимания между народами и странами. Мы верим, что эти меры откроют путь к дальнейшему развитию общества, действительно основанного на знаниях.

Документ WSIS-03/GENEVA/DOC/5-R
12 декабря 2003 года
Оригинал: английский

План действий

A. Введение

1. В настоящем Плане действий общая концепция и руководящие принципы Декларации находят свое воплощение в конкретных направлениях деятельности, которые ведут к достижению согласованных на международном уровне целей развития, в том числе содержащихся в Декларации тысячелетия, Монтеррейском консенсусе и йоханнесбургских Декларации и Плане выполнения решений, путем содействия применению продуктов, сетей, услуг и приложений на базе ИКТ, а также призваны помочь странам в преодолении разрыва в цифровых технологиях. Информационное общество, создание которого предусматривается в Декларации принципов, будет строиться, в условиях сотрудничества и солидарности, органами государственного управления и всеми другими заинтересованными сторонами.

2. Информационное общество — это эволюционирующая структура, которая, отражая различные стадии развития, достигла разных уровней в разных странах мира. Технологический прогресс и прочие изменения стремительно преобразуют среду, в которой развивается информационное общество. В связи с этим План действий представляет собой эволюционирующую основу, обеспечивающую продвижение к информационному обществу на национальном, региональном и международном уровнях. Уникальная двухэтапная структура Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО) позволяет учитывать подобную эволюцию.

3. Всем заинтересованным сторонам предстоит сыграть важную роль в информационном обществе, прежде всего через партнерские отношения:

a) органам государственного управления принадлежит ведущая роль в разработке и осуществлении всеобъемлющих, перспективных и устойчивых национальных электронных стратегий. Частный сектор и гражданское общество, в диалоге с органами государственного управления, должны сыграть важную консультативную роль в формировании национальных электронных стратегий;

b) участие частного сектора имеет большое значение для развития и распространения информационных и коммуникационных технологий (ИКТ), для инфраструктуры, контента и приложений. Частный сектор не только является участником рынка, но и играет определенную роль в более широком контексте устойчивого развития;

c) участие и заинтересованность гражданского общества столь же важны для создания справедливого информационного общества и осуществления инициатив в области развития, относящихся к ИКТ;

d) международные и региональные учреждения, в том числе международные финансовые учреждения, играют ключевую роль в интеграции применения ИКТ в про-

цесс развития и в предоставлении необходимых ресурсов для построения информационного общества и оценки достигнутого прогресса в этой области.

B. Задачи, цели и контрольные показатели

4. Задачи Плана действий состоят в том, чтобы построить открытое для всех информационное общество; поставить потенциал, заключенный в знаниях и ИКТ, на службу развитию; способствовать использованию информации и знаний для достижения согласованных на международном уровне целей развития, в том числе содержащихся в Декларации тысячелетия; и решать новые проблемы информационного общества на национальном, региональном и международном уровнях. На втором этапе ВВУИО следует воспользоваться возможностью для анализа и оценки прогресса, достигнутого в ликвидации разрыва в цифровых технологиях.

5. На национальном уровне в рамках национальных электронных стратегий и в соответствии с государственной политикой в области развития в надлежащих случаях должны быть установлены конкретные контрольные показатели построения информационного общества с учетом национальных особенностей. Такие контрольные показатели могут служить полезными вехами для осуществляемых действий и оценки прогресса в достижении общих целей информационного общества.

6. Основанные на согласованных на международном уровне целях в области развития, в том числе содержащихся в Декларации тысячелетия, которые базируются на международном сотрудничестве, ориентировочные контрольные показатели могут служить глобальными целевыми показателями роста уровня подключения и доступа при применении ИКТ в рамках выполнения задач Плана действий, которые должны быть реализованы к 2015 году. Эти контрольные показатели могут приниматься во внимание при установлении национальных контрольных показателей с учетом национальных особенностей:

a) обеспечить подключением на базе ИКТ деревни и создать в них пункты коллективного доступа;

b) обеспечить подключением на базе ИКТ университеты, колледжи, средние и начальные школы;

c) обеспечить подключением на базе ИКТ научно-исследовательские центры;

d) обеспечить подключением на базе ИКТ публичные библиотеки, культурные центры, музеи, почтовые отделения и архивы;

e) обеспечить подключением на базе ИКТ центры здравоохранения и больницы;

f) обеспечить подключением все местные и центральные государственные учреждения и обеспечить наличие у них Webсайтов и адресов электронной почты;

g) внести изменения в программы всех начальных и средних школ, с тем чтобы включить в них задачи, выдвинутые информационным обществом, с учетом национальных особенностей;

h) обеспечить все население планеты доступом к службам теле— и радиовещания;

i) поощрять развитие контента и создать технические условия, которые способствовали бы представлению и использованию в Интернет всех языков мира;

j) обеспечить доступ к ИКТ в пределах досягаемости более чем для половины населения планеты.

7. При решении этих задач и достижении целей и контрольных показателей особое внимание должно уделяться потребностям развивающихся стран, в частности стран, народов и групп, упоминаемых в пунктах 11–16 Декларации принципов.

C. Направления действий

C1. Роль органов государственного управления и всех заинтересованных сторон в содействии применению ИКТ в целях развития

8. Решающее значение для развития информационного общества имеет действенное участие органов государственного управления и всех заинтересованных сторон, для чего необходимы сотрудничество и партнерские отношения между всеми ними.

a) Все страны должны поощрять разработку к 2005 году национальных электронных стратегий, включая наращивание необходимого человеческого потенциала, с учетом национальных особенностей.

b) Приступить на национальном уровне к организованному диалогу с участием всех заинтересованных сторон, в том числе в рамках партнерских отношений между государственным и частным секторами, относительно разработки электронных стратегий для информационного общества и обмена образцами наилучшей практики.

c) При разработке и осуществлении национальных электронных стратегий заинтересованные стороны должны учитывать местные, региональные и национальные потребности и проблемы. Для получения максимальных преимуществ от осуществляемых инициатив в них необходимо включать принцип устойчивости. Частный сектор должен принимать участие в конкретных проектах развития информационного общества на местном, региональном и национальном уровнях.

d) Каждая страна призвана создать к 2005 году по крайней мере одно действующее партнерство между государственным и частным секторами (ПГЧ) или партнерство между несколькими секторами (ПНС) в качестве образца для дальнейшей деятельности.

e) Определить на национальном, региональном и международном уровнях механизмы, необходимые для установления и развития партнерских отношений между заинтересованными сторонами в информационном обществе.

f) Изучить целесообразность создания на национальном уровне порталов для коренных народов с участием различных заинтересованных сторон.

g) К 2005 году соответствующие международные организации и финансовые учреждения должны разработать собственные стратегии применения ИКТ в целях устойчивого развития, в том числе относящиеся к устойчивым схемам производства и потребления; эти стратегии должны стать также эффективным инструментом содействия достижению целей, установленных Организацией Объединенных Наций в Декларации тысячелетия.

h) Международные организации должны публиковать, в том числе на своих Web-сайтах, относящуюся к сфере их компетенции и представленную соответствующими заинтересованными сторонами достоверную информацию об успешно проведенных мероприятиях по включению ИКТ в основные направления деятельности.

i) Содействовать осуществлению ряда связанных с этим мер, в том числе созданию схем бизнес-инкубаторов, предоставлению венчурного капитала (на национальном и международном уровнях), учреждению государственных инвестиционных фондов, в том числе для микрофинансирования малых, средних и микропредприятий (МСМП), реализации стратегии привлечения инвестиций, проведению мероприятий в поддержку экспорта программного обеспечения (торгового консультирования), поддержке сетей для проведения научно-исследовательских и опытно-конструкторских работ и парков программного обеспечения.

C2. Информационная и коммуникационная инфраструктура — необходимый фундамент информационного общества

9. Инфрастуктура является основой для достижения цели по охвату всех жителей планеты цифровыми технологиями, то есть предоставления универсального, устойчивого, повсеместного и приемлемого в ценовом отношении доступа к ИКТ для всех, с учетом соответствующих решений, уже применяемых в развивающихся странах и странах с переходной экономикой, для обеспечения надежного подключения и доступа к отдаленным и маргинализированным районам на национальном и региональном уровнях.

a) Органы государственного управления в рамках национальной политики развития должны принимать решения, направленные на поддержку благоприятной и кон-

курентной среды для получения необходимых инвестиций в инфраструктуру ИКТ и для развития новых услуг.

b) Выработать в рамках национальных электронных стратегий соответствующие политику и стратегию обеспечения универсального доступа и определить средства их реализации, согласно ориентировочным контрольным показателям, а также разработать показатели доступа к ИКТ.

c) В рамках национальных электронных стратегий, согласно ориентировочным контрольным показателям, обеспечить и совершенствовать подключение на базе ИКТ всех школ, университетов, учреждений здравоохранения, библиотек, почтовых отделений, общинных центров, музеев и других доступных для населения учреждений.

d) Развивать и укреплять инфраструктуру национальных, региональных и международных сетей широкополосной связи, включая спутниковые и другие системы, для содействия обеспечению пропускной способности, отвечающей потребностям стран и их граждан, а также создающей условия для предоставления новых услуг на базе ИКТ. Оказывать поддержку техническим, регламентарным и эксплуатационным исследованиям, проводимым Международным союзом электросвязи (МСЭ) и, в надлежащих случаях, другими соответствующими международными организациями, с тем чтобы:

i) расширить доступ к орбитальным ресурсам, обеспечить глобальную гармонизацию использования частот и глобальную стандартизацию систем;

ii) поощрять партнерские отношения между государственным и частным секторами;

iii) содействовать оказанию глобальных услуг высокоскоростной спутниковой связи для районов, обслуживаемых в недостаточной степени, в частности отдаленных и малонаселенных районов;

iv) исследовать другие системы, способные обеспечивать высокоскоростные подключения.

e) В рамках национальных электронных стратегий добиваться удовлетворения особых потребностей престарелых, лиц с ограниченными возможностями, детей, прежде всего маргинализированных детей, а также других уязвимых и находящихся в неблагоприятном положении групп населения, в том числе с помощью соответствующих мер образовательного, административного и законодательного характера, направленных на обеспечение полномасштабного включения указанных групп в информационное общество.

f) Поощрять разработку и производство оборудования и услуг на базе ИКТ, удобных в использовании и приемлемых в ценовом отношении для всех, включая престарелых, лиц с ограниченными возможностями, детей, прежде всего маргинализированных детей, равно как и другие уязвимые и находящиеся в неблагоприятном положении группы населения, а также содействовать развитию технологий, приложений и контента, в соответствии с их потребностями, на основе принципов универсального дизайна и при дальнейшем совершенствовании путем использования ассистивных технологий.

g) В целях смягчения проблем, связанных с неграмотностью, разработать приемлемые в ценовом отношении технологии и бестекстовые компьютерные интерфейсы, с тем чтобы облегчить людям доступ к ИКТ.

h) На международном уровне проводить научно-исследовательские и опытно-конструкторские работы, направленные на создание надлежащего и приемлемого в ценовом отношении оборудования на базе ИКТ для конечных пользователей.

i) Поощрять использование, в развитых странах и в особенности в развивающихся странах, неиспользуемых мощностей беспроводной связи, включая спутниковую связь, для обеспечения доступа в отдаленных районах, в первую очередь в развивающихся

странах и странах с переходной экономикой, а также для более широкого внедрения низкозатратного подключения в развивающихся странах. Особое внимание следует уделять наименее развитым странам (НРС), стремящимся создать инфраструктуру электросвязи.

j) Оптимизировать соединения между основными информационными сетями, поощряя создание и развитие региональных магистральных структур на базе ИКТ и коммутационных станций Интернет для снижения стоимости межсетевых соединений и расширения доступа к сетям.

k) Разрабатывать стратегии распространения в глобальном масштабе приемлемого в ценовом отношении подключения, способствуя тем самым совершенствованию доступа. Устанавливаемые на коммерческой основе затраты на транзит и межсетевые соединения через Интернет должны базироваться на объективных, прозрачных и не допускающих дискриминации параметрах с учетом ведущейся по этой теме работы.

l) Поощрять и стимулировать совместное использование традиционных средств массовой коммуникации и новых технологий.

С3. Доступ к информации и знаниям

10. ИКТ дают людям возможность получать доступ к информации и знаниям практически мгновенно в любой точке планеты. Благами доступа к знаниям и информации должны пользоваться частные лица, организации и общины.

a) Разрабатывать политические руководящие принципы для развития и популяризации информации, являющейся публичным достоянием, как важный международный инструмент содействия доступу населения к информации.

b) Органы государственного управления призваны обеспечить посредством различных ресурсов связи, в первую очередь Интернет, надлежащий доступ к официальной информации, являющейся публичным достоянием. Поощряется разработка законодательства относительно доступа к информации и сохранения являющихся публичным достоянием данных, особенно в области новых технологий.

c) Поддерживать научно-исследовательские и опытно-конструкторские работы, с тем чтобы содействовать доступности ИКТ для всех, в том числе для находящихся в неблагоприятных условиях, маргинализированных и уязвимых групп населения.

d) Органам государственного управления и другим заинтересованным сторонам следует создавать устойчиво функционирующие многоцелевые публичные пункты коллективного доступа, предоставляющие для граждан по приемлемым ценам или бесплатно доступ к различным ресурсам связи, в первую очередь Интернет. Эти пункты доступа должны, по мере возможности, обладать достаточной пропускной способностью для оказания помощи пользователям в библиотеках, учебных заведениях, государственных структурах, почтовых отделениях и прочих общественных местах, причем особое внимание следует уделять сельским и обслуживаемым в недостаточной степени районам, при соблюдении прав интеллектуальной собственности (ПИС) и поощрении использования информации и обмена знаниями.

e) Поощрять исследования и содействовать осведомленности всех заинтересованных сторон о возможностях, предоставляемых различными моделями программного обеспечения, и о средствах его создания, включая программное обеспечение, разрабатываемое отдельными компаниями, программное обеспечение с открытыми кодами и свободно распространяемое программное обеспечение, с тем чтобы расширять конкуренцию и разнообразие выбора, повышать ценовую приемлемость и дать всем заинтересованным сторонам возможность понять, какой вариант является для них наиболее подходящим.

f) Правительства должны активно содействовать применению гражданами своих стран и местными органами власти ИКТ в качестве основного рабочего инструмента. Для достижения этой цели международному сообществу и другим заинтересованным

сторонам следует поддерживать — в качестве средства совершенствования местного управления — наращивание потенциала местных органов власти на основе широкого использования ИКТ.

g) Поощрять исследования по вопросам информационного общества, в том числе по инновационным формам создания сетей, адаптации инфраструктуры ИКТ, инструментов и приложений на базе ИКТ, содействующим доступности ИКТ для всех, в частности для групп населения, находящихся в неблагоприятном положении.

h) Поддерживать создание и развитие публичной библиотечной и архивной цифровой службы, адаптированной к информационному обществу, в том числе путем пересмотра национальных стратегий и законодательства в области библиотечного обслуживания, обеспечения на глобальном уровне понимания потребности в «гибридных библиотеках» и способствуя сотрудничеству библиотек на всемирном уровне.

i) Поощрять инициативы по содействию доступу, в том числе свободному и приемлемому в ценовом отношении доступу к находящимся в открытом доступе журналам и книгам и открытым архивам научной информации.

j) Поддерживать научно-исследовательские и опытно-конструкторские работы в области проектирования полезных инструментов для всех заинтересованных сторон с целью повышения осведомленности, проведения анализа и оценки различных моделей программного обеспечения и соответствующего лицензирования, с тем чтобы обеспечить оптимальный выбор надлежащего программного обеспечения, которое бы наилучшим образом способствовало достижению целей развития в местных условиях.

С4. Наращивание потенциала

11. Каждый должен обладать навыками, необходимыми для использования в полной мере преимуществ информационного общества. Поэтому следует наращивать потенциал и повышать грамотность в сфере ИКТ. ИКТ могут способствовать достижению во всемирном масштабе всеобщего образования путем предоставления средств получения образования и подготовки преподавателей, создания более совершенных условий для обучения на протяжении всей жизни, которое охватывало бы людей, находящихся вне рамок формальной системы образования, а также для совершенствования профессиональных навыков.

a) Разрабатывать национальные стратегии для обеспечения полномасштабной интеграции ИКТ в сферу образования и профессиональной подготовки на всех уровнях, в том числе в разработку учебных программ, подготовку преподавателей, управление и руководство учреждениями, равно как и в поддержку обучения на протяжении всей жизни.

b) Разрабатывать программы ликвидации неграмотности при помощи ИКТ на национальном, региональном и международном уровнях и содействовать их внедрению.

c) Содействовать всем в овладении навыками электронной грамотности, например путем разработки и организации курсов для государственных служащих, используя для этого такие существующие структуры, как библиотеки, многоцелевые общинные центры, публичные пункты доступа, а также путем создания на местах центров профессиональной подготовки в области ИКТ в сотрудничестве со всеми заинтересованными сторонами. Особое внимание следует уделять находящимся в неблагоприятном положении и уязвимым группам населения.

d) В контексте национальной политики в области образования и с учетом необходимости ликвидации неграмотности среди взрослых обеспечить, чтобы молодежь была вооружена знаниями и навыками применения ИКТ, в том числе обладала способностью творчески и новаторски анализировать и обрабатывать информацию, делиться своим опытом и в полной мере участвовать в информационном обществе.

e) Органы государственного управления, в сотрудничестве с другими заинтересованными сторонами, должны разрабатывать программы наращивания потенциала, в которых основное внимание уделялось бы созданию критической массы квалифицированных и опытных профессионалов и экспертов в области ИКТ.

f) Разрабатывать экспериментальные проекты для демонстрации воздействия альтернативных систем образования на базе ИКТ, в первую очередь для достижения целей образования для всех, в том числе целей обеспечения базовой грамотности.

g) Работать над устранением гендерных барьеров к получению образования и профессиональной подготовки в области ИКТ и содействовать обеспечению равных возможностей профессиональной подготовки в связанных с ИКТ областях для женщин и девочек. Программы, осуществляемые в области науки и техники, с самого начала должны быть ориентированы на девочек, чтобы увеличить число женщин, занятых в сфере ИКТ. Содействовать обмену образцами наилучшей практики по включению принципа равноправия мужчин и женщин в образование в области ИКТ.

h) Давать местным общинам, в первую очередь в сельских и в недостаточной степени обслуживаемых районах, возможность применять ИКТ и обеспечивать производство полезного и социально значимого контента для всеобщего блага.

i) Приступить к осуществлению программ в области образования и профессиональной подготовки, используя, где это возможно, информационные сети исконно кочевых и коренных народностей, чтобы открыть им возможность в полной мере участвовать в информационном обществе.

j) Планировать и осуществлять на региональном и международном уровнях совместные мероприятия с целью развития потенциала, прежде всего руководителей и эксплуатационного персонала в развивающихся странах и НРС, для эффективного применения ИКТ на всех направлениях образовательной деятельности. При этом следует предусматривать и обучение вне рамок образовательной системы, например на рабочем месте и дома.

k) Разрабатывать специальные программы профессиональной подготовки по применению ИКТ для удовлетворения потребностей в обучении специалистов в сфере информации, таких как архивные, библиотечные и музейные работники, ученые, преподаватели, журналисты, почтовые служащие и другие соответствующие профессиональные группы. При подготовке специалистов в области информации следует опираться не только на новые методы и способы, предназначенные для развития и оказания информационных и коммуникационных услуг, но и на соответствующие навыки управления, с тем чтобы обеспечить оптимальное применение технологий. При подготовке преподавателей основное внимание следует уделять техническим аспектам ИКТ, разработке контента и возможностям и перспективам, которые открывают ИКТ.

l) Развивать дистанционные обучение, профессиональную подготовку и другие формы обучения и профессиональной подготовки как часть программ наращивания потенциала. Уделять особое внимание развивающимся странам, и прежде всего НРС, с различными уровнями развития людских ресурсов.

m) Содействовать международному и региональному сотрудничеству в области наращивания потенциала, в том числе осуществлению страновых программ, разрабатываемых Организацией Объединенных Наций и ее специализированными учреждениями.

n) Осуществлять экспериментальные проекты для разработки новых форм сетевой работы на базе ИКТ, которые соединяли бы педагогические и профессионально-технические учебные заведения и научно-исследовательские учреждения в развитых и развивающихся странах и странах с переходной экономикой.

o) Движение добровольцев, если оно действует в соответствии с национальной политикой и местными культурными традициями, может быть ценным средством как

для повышения способности людских ресурсов продуктивно использовать инструменты на базе ИКТ, так и для построения более открытого для всех информационного общества. Организовывать добровольческие программы для наращивания потенциала в области ИКТ в целях развития, прежде всего в развивающихся странах.

p) Разрабатывать программы для обучения пользователей методам развития потенциала самообразования и саморазвития.

C5. Укрепление доверия и безопасности при использовании ИКТ

12. Доверие и безопасность относятся к главным опорам информационного общества.

a) Содействовать сотрудничеству между государствами в рамках Организации Объединенных Наций и со всеми заинтересованными сторонами в рамках соответствующих форумов с целью укрепления доверия пользователей, повышения надежности и защиты целостности как данных, так и сетей; анализа существующих и потенциальных угроз в области ИКТ; а также решения других вопросов информационной безопасности и безопасности сетей.

b) Органам государственного управления в сотрудничестве с частным сектором необходимо предупреждать, обнаруживать проявления киберпреступности и ненадлежащего использования ИКТ и реагировать на эти проявления путем разработки руководящих принципов, которые учитывали бы ведущуюся в этой области работу; изучения законодательства, которое дает возможность эффективно расследовать и подвергать преследованию ненадлежащее использование; содействия эффективным мерам взаимопомощи; усиления на международном уровне институциональной поддержки профилактики таких инцидентов, их обнаружения и ликвидации их последствий; а также путем содействия образованию и повышению осведомленности.

c) Органы государственного управления и другие заинтересованные стороны должны активно поощрять обучение пользователей и повышать их осведомленность относительно неприкосновенности частной жизни при работе в онлайновом режиме и способов ее защиты.

d) Принимать необходимые меры на национальном и международном уровнях для защиты от спама.

e) Поощрять проведение на национальном уровне оценки внутреннего законодательства с целью ликвидации препятствий для эффективного использования документов и осуществления сделок в электронной форме, в том числе использования электронных методов аутентификации.

f) Продолжать укрепление надежности и безопасности с помощью взаимодополняющих и взаимоусиливающих инициатив в сфере безопасности при использовании ИКТ и инициатив или руководящих принципов в отношении прав на неприкосновенность частной жизни, защиту данных и прав потребителей.

g) Обмениваться образцами наилучшей практики в области информационной безопасности и безопасности сетей и поощрять их использование всеми заинтересованными сторонами.

h) Предложить заинтересованным странам назначить координаторов для реагирования в режиме реального времени на происшествия в сфере безопасности и объединить этих координаторов в открытую совместную сеть для обмена информацией и технологиями реагирования на происшествия.

i) Поощрять дальнейшее развитие безопасных и надежных приложений для упрощения осуществления сделок в онлайновом режиме.

j) Поощрять активное участие заинтересованных стран в проводимой Организацией Объединенных Наций деятельности по укреплению доверия и надежности при использовании ИКТ.

С6. Благоприятная среда

13. Для достижения максимальных преимуществ информационного общества в социальной, экономической и экологической сферах органам государственного управления необходимо создавать надежную, прозрачную, недискриминационную правовую, регламентарную и политическую среду. Для этого:

a) Органы государственного управления должны способствовать созданию благоприятных, прозрачных, содействующих развитию конкуренции и предсказуемых политических, правовых и регламентарных рамок, которые обеспечивали бы надлежащие стимулы для инвестиций и развития общин в информационном обществе.

b) Мы обращаемся к Генеральному секретарю Организации Объединенных Наций с просьбой учредить рабочую группу по управлению использованием Интернет в рамках открытого и всеобъемлющего процесса, обеспечивающего механизм для полномасштабного и активного участия органов государственного управления, частного сектора и гражданского общества как из развивающихся, так и из развитых стран, в том числе соответствующих межправительственных и международных организаций и форумов, в целях изучения вопроса об управлении использованием Интернет и представления к 2005 году предложений для принятия решения в отношении организации управления использованием Интернет. В частности группе следует:

i) выработать рабочее определение управления использованием Интернет;

ii) выявить вопросы государственной политики, которые относятся к управлению использованием Интернет;

iii) сформировать единое понимание соответствующей роли и сферы ответственности органов государственного управления, существующих межправительственных и международных организаций и других форумов, а также частного сектора и гражданского общества как из развивающихся, так и из развитых стран;

iv) подготовить отчет о результатах проделанной работы для представления на рассмотрение в ходе второго этапа ВВУИО в Тунисе в 2005 году и принятия соответствующего решения.

c) Органам государственного управления предлагается:

i) содействовать созданию национальных и региональных коммутационных центров Интернет;

ii) осуществлять в надлежащих случаях управление своими соответствующими доменами высшего уровня, имеющими код страны (ccTLD), или надзор за ними;

iii) повышать уровень информированности об использовании Интернет.

d) В сотрудничестве с соответствующими заинтересованными сторонами содействовать созданию региональных корневых серверов и использованию интернационализированных наименований доменов, с тем чтобы преодолеть препятствующие доступу барьеры.

e) Органам государственного управления следует продолжать обновлять национальные законы по защите прав потребителей, приводя их в соответствие с новыми требованиями информационного общества.

f) Содействовать эффективному участию развивающихся стран и стран с переходной экономикой в международных форумах по вопросам ИКТ и создавать возможности для обмена опытом.

g) Органам государственного управления необходимо разработать национальные стратегии, в том числе стратегии электронного государственного управления, с тем чтобы сделать государственное управление более прозрачным, эффективным и демократичным.

h) Разработать основу для безопасного хранения и архивирования документов и других электронных информационных записей.

i) Органы государственного управления и заинтересованные стороны должны активно содействовать просвещению пользователей и информированию их относительно неприкосновенности частной жизни при работе в онлайновом режиме и способов защиты неприкосновенности частной жизни.

j) Предложить заинтересованным сторонам обеспечить, чтобы меры, разработанные в целях содействия электронной торговле, давали потребителям также возможность выбора: использовать электронную связь или отказаться от нее.

k) Поощрять ведущуюся работу в области создания эффективных систем разрешения споров, в частности по введению альтернативных методов разрешения споров (АМР), которые могут способствовать разрешению споров.

l) Органам государственного управления в сотрудничестве с заинтересованными сторонами предлагается разрабатывать политику в области ИКТ, благоприятную для развития предпринимательства, содействия инновациям и инвестициям, уделяя при этом особое внимание расширению участия женщин.

m) С учетом экономического значения ИКТ для малых и средних предприятий (МСП) следует помогать им повышать свою конкурентоспособность, упрощая административные процедуры, обеспечивая им доступ к финансовым ресурсам и повышая их способность участвовать в связанных с ИКТ проектах.

n) Органы государственного управления должны быть образцовыми пользователями и лидерами в переходе к электронной торговле в соответствии с уровнем социально-экономического развития своих стран.

o) Органы государственного управления в сотрудничестве с другими заинтересованными сторонами должны повышать информированность о значении международных стандартов функциональной совместимости для глобальной электронной торговли.

p) Органы государственного управления в сотрудничестве с другими заинтересованными сторонами должны содействовать разработке и применению открытых, обеспечивающих возможность взаимодействия, недискриминационных и определяемых спросом стандартов.

q) МСЭ, используя свой потенциал договорных отношений, координирует использование и осуществляет распределение частот в интересах содействия повсеместному и приемлемому в ценовом отношении доступу.

r) В рамках МСЭ и других региональных организаций следует принимать дополнительные меры для обеспечения рационального, эффективного и экономичного использования всеми странами радиочастотного спектра, а также справедливого доступа к нему на основе соответствующих международных соглашений.

С7. Приложения на базе ИКТ: преимущества во всех аспектах жизни

14. Приложения на базе ИКТ могут служить опорой для устойчивого развития в сферах государственного управления, хозяйственной деятельности, образования и профессиональной подготовки, здравоохранения, занятости, окружающей среды, сельского хозяйства и науки в рамках национальных электронных стратегий. Сюда можно отнести действия в следующих секторах:

15. **Электронное государственное управление**

a) Осуществлять стратегии электронного государственного управления, уделяя основное внимание приложениям, направленным на обеспечение инновационной деятельности и прозрачности государственных учреждений и демократических процессов, повышая эффективность и укрепляя связи с гражданами.

b) Разрабатывать на всех уровнях национальные инициативы и услуги электронного государственного управления, соответствующие потребностям граждан и деловых кругов, с тем чтобы добиться более эффективного распределения ресурсов и публичного достояния.

c) Поддерживать инициативы по международному сотрудничеству в области электронного государственного управления в целях повышения прозрачности, подотчетности и эффективности на всех уровнях государственного управления.

16. Электронная коммерческая деятельность

a) Органы государственного управления, международные организации и частный сектор призваны популяризировать преимущества международной торговли и содействовать ведению электронной коммерческой деятельности, а также использованию в развивающихся странах и странах с переходной экономикой моделей электронной коммерческой деятельности.

b) Органам государственного управления следует посредством создания благоприятной среды и на основе получившего повсеместное распространение доступа к Интернет стимулировать инвестиции со стороны частного сектора, поощрять создание новых приложений и разработку контента, а также способствовать сотрудничеству государственного и частного секторов.

c) Политика органов государственного управления должна быть направлена на поддержку и развитие МСМП в отрасли ИКТ, а также на содействие их участию в электронной коммерческой деятельности, с тем чтобы стимулировать экономический рост и создание новых рабочих мест в рамках стратегии сокращения уровня бедности посредством создания материальных благ.

17. Электронное обучение (см. раздел C4)

18. Электронное здравоохранение

a) Поощрять совместные действия органов государственного управления, планирующих органов, специалистов в области здравоохранения, а также других учреждений наряду с участием международных организаций в создании надежных, работающих без задержек, высококачественных и доступных в ценовом отношении систем здравоохранения и информационных систем по охране здоровья, а также в содействии постоянной профессиональной подготовке, образованию и исследованиям в области медицины с помощью ИКТ, при этом соблюдая и защищая право граждан на неприкосновенность частной жизни.

b) Содействовать доступу к существующим в мире медицинским знаниям и актуальным на местном уровне информационным ресурсам для укрепления государственных исследовательских и профилактических программ в области здравоохранения и охраны здоровья мужчин и женщин, в частности к информации о сексуальном и репродуктивном здоровье и инфекциях, передаваемых половым путем, а также о заболеваниях, на которые обращено внимание всего мира, таких как ВИЧ/СПИД, малярия и туберкулез.

c) Проводить профилактику, мониторинг и контроль за распространением инфекционных заболеваний, совершенствуя для этого коллективные информационные системы.

d) Содействовать разработке международных стандартов для обмена медицинскими данными, уделяя при этом должное внимание обеспечению неприкосновенности частной жизни.

e) Поощрять применение ИКТ для повышения качества и расширения охвата здравоохранением и информационной системой охраны здоровья в отдаленных и обслуживаемых в недостаточной степени районах, а также в интересах уязвимых групп населения, признавая при этом роль женщин в оказании медицинской помощи в семьях и общинах.

f) Укреплять и расширять инициативы на базе ИКТ по предоставлению медицинской и гуманитарной помощи при бедствиях и в чрезвычайных ситуациях.

19. Электронная занятость

a) Поощрять на национальном уровне создание для работников и работодателей, применяющих электронные формы труда, образцов наилучшей практики на основе

принципов справедливости и равноправия женщин и мужчин, соблюдая при этом все соответствующие международные нормы.

b) Популяризировать новые способы организации работы и коммерческой деятельности с целью повышения производительности, содействия экономическому росту и росту благосостоянию путем инвестиций в ИКТ и людские ресурсы.

c) Поощрять применение телеработы, позволяющей гражданам, и прежде всего в развивающихся странах, НРС и малых странах жить в своем обществе, работая при этом в любом месте, а также расширять возможности трудоустройства для женщин и лиц с ограниченными возможностями. Популяризируя телеработу, особое внимание следует уделять стратегиям, способствующим созданию рабочих мест и сохранению квалифицированной рабочей силы.

d) Способствовать введению с самого начала ориентированных на девушек программ в научно-технической области с целью увеличения числа женщин, работающих в сфере ИКТ.

20. Электронная охрана окружающей среды

a) Органы государственного управления в сотрудничестве с другими заинтересованными сторонами призваны использовать и пропагандировать ИКТ как инструмент для охраны окружающей среды и устойчивого использования природных ресурсов.

b) Органы государственного управления, гражданское общество и частный сектор призваны выступать инициаторами мер и осуществлять проекты и программы устойчивого производства и потребления и экологически безопасной утилизации и рециклирования вышедшего из употребления аппаратного обеспечения и деталей оборудования на базе ИКТ.

c) Создавать системы контроля на базе ИКТ для прогнозирования и мониторинга воздействия на окружающую среду стихийных и антропогенных катастроф, в особенности в развивающихся странах, НРС и малых странах.

21. Электронное сельское хозяйство

a) Обеспечивать систематическое распространение на базе ИКТ информации по сельскому хозяйству, животноводству, рыбному промыслу, лесному хозяйству и продовольствию с целью предоставления свободного доступа к комплексным, актуальным и подробным знаниям и информации, особенно в сельских районах.

b) В партнерствах государственного и частного секторов следует стремиться максимально расширять использование ИКТ как инструмента для совершенствования производства (в количественном и качественном отношении).

22. Электронная научная деятельность

a) Содействовать тому, чтобы все университеты и научно-исследовательские институты имели приемлемое в ценовом отношении и надежное высокоскоростное подключение к Интернет в целях обеспечения их решающей роли в производстве информации и знаний, образовании и профессиональной подготовке и содействовать налаживанию партнерских отношений, сотрудничества и сетевой связи между этими учреждениями.

b) Стимулировать инициативы в области электронной издательской деятельности, дифференцированного ценообразования и открытого доступа, с тем чтобы научная информация была приемлемой в ценовом отношении и доступной на справедливой основе во всех странах.

c) Содействовать применению одноранговой технологии для совместного использования научных знаний, препринтов и перепечаток трудов ученых, отказавшихся от своего права на гонорары.

d) Содействовать в долгосрочной перспективе систематическому и эффективному сбору, распространению и сохранности важнейших научных данных в цифровой форме, например демографических и метеорологических данных, во всех странах.

e) Популяризировать принципы и стандарты метаданных для содействия сотрудничеству и эффективному использованию собранной научной информации и данных, как это требуется для проведения научных исследований.

C8. Культурное разнообразие и культурная самобытность, языковое разнообразие и местный контент

23. Культурное и языковое разнообразие, стимулирующее уважение культурной самобытности, традиций и религий, является необходимым условием развития информационного общества на базе диалога между культурами и регионального и международного сотрудничества. Оно представляет собой важный фактор устойчивого развития.

a) Разрабатывать политику, способствующую уважению, сохранению, развитию и укреплению культурного и языкового разнообразия и культурного наследия в рамках информационного общества, что отражено в соответствующих принятых Организацией Объединенных Наций документах, в том числе во Всеобщей декларации ЮНЕСКО о культурном разнообразии. В частности, необходимо побуждать органы государственного управления разрабатывать политику в области культуры для содействия производству культурного, образовательного и научного контента и развития на местном уровне отраслей культуры, соответствующих языковым и культурным особенностям пользователей.

b) Разрабатывать национальные политику и законодательство, благодаря которым библиотеки, архивы, музеи и другие учреждения культуры в информационном обществе могли бы в полной мере выполнять свою функцию поставщиков контента — в том числе традиционных знаний, — в частности обеспечивая постоянный доступ к записанной информации.

c) Поддерживать усилия по разработке и применению ИКТ для сохранения природного и культурного наследия, обеспечивать доступ к нему как к живой части современной культуры. Для этого необходимо разрабатывать системы обеспечения постоянного доступа к архивированной информации в цифровой форме и мультимедийному контенту в цифровых хранилищах, а также оказывать поддержку архивам, собраниям предметов культуры и библиотекам как памяти человечества.

d) Разрабатывать и осуществлять политику, которая способствовала бы сохранению, укреплению, уважению и развитию многообразия культур, знаний и традиций коренных народов посредством создания разнообразного информационного контента и применения различных методов, в том числе перевода в цифровую форму наследия в области образования, науки и культуры.

e) Поддерживать деятельность местных органов власти по разработке, переводу и адаптации местного контента, созданию архивов в цифровой форме и обеспечению разнообразия форм цифровых и традиционных средств массовой информации. Эти виды деятельности могут также способствовать укреплению местных и коренных общин.

f) Посредством доступа к услугам традиционных и цифровых средств массовой информации обеспечить наличие контента, актуального в культурном и лингвистическом аспектах для составляющих информационное общество людей.

g) Посредством установления партнерских отношений между государственным и частным секторами ускорять создание разнообразного местного и национального контента, в том числе доступного на языках пользователей, а также признавать и поддерживать работу на базе ИКТ во всех областях искусства.

h) Расширять в системах формального и неформального образования для всех учебные программы, учитывающие гендерные аспекты, и повышать грамотность женщин в области связи и СМИ, с тем чтобы наращивать потенциал девочек и женщин в отношении разработки контента ИКТ.

i) Развивать существующий на местах потенциал для разработки и распространения программного обеспечения на местных языках, а также контента, актуального для различных слоев населения, в том числе неграмотных, лиц с ограниченными возможностями, находящихся в неблагоприятном положении и уязвимых групп населения, в особенности в развивающихся странах и странах с переходной экономикой.

j) Оказывать поддержку средствам массовой информации местных общин и поддерживать проекты, в которых сочетается применение традиционных СМИ и новых технологий в интересах более широкого использования местных языков, документирования и сохранения местного наследия, включая ландшафтное и биологическое разнообразие, и в качестве средства, обеспечивающего охват сельских, изолированных и кочевых общин.

k) Укреплять потенциал коренных народов по развитию контента на их родных языках.

l) Сотрудничать с коренными народами и традиционными общинами, с тем чтобы в информационном обществе они могли более эффективно применять свои традиционные знания и получать от этого выгоду.

m) Осуществлять обмен знаниями, опытом и образцами наилучшей практики, относящимися к политике и инструментам, направленным на содействие культурному и языковому разнообразию на региональном и субрегиональном уровнях. Этого можно добиться путем создания, для содействия предпринимаемым в целях интеграции усилиям, региональных и субрегиональных рабочих групп по конкретным вопросам настоящего Плана действий.

n) Проводить на региональном уровне оценку вклада ИКТ в культурный обмен и взаимодействие и на основании результатов этой оценки разрабатывать соответствующие программы.

o) Органы государственного управления, в рамках партнерских отношений между государственным и частным секторами, должны содействовать распространению технологий и осуществлению программ НИОКР в таких областях, как письменный перевод, иконография и услуги на базе речевой связи, а также развитию моделей необходимого аппаратного и разнообразного программного обеспечения, в том числе программного обеспечения, разрабатываемого отдельными компаниями, программного обеспечения с открытыми кодами и свободно распространяемого программного обеспечения, такого как стандартные наборы символов, языковые коды, электронные словари, терминологические справочники и тезаурусы, многоязычные поисковые машины, инструменты машинного перевода, интернационализированные наименования доменов, снабжение контента ссылками, а также общего и прикладного программного обеспечения.

C9. Средства массовой информации

24. Средства массовой информации — в своих различных видах и при многообразии форм собственности — в качестве действующего фактора играют существенную роль в развитии информационного общества и признаны важным выразителем свободы слова и плюрализма информации.

a) Поощрять СМИ — печатные и электронные, а также новые виды СМИ — к тому, чтобы они и далее играли важную роль в информационном обществе.

b) Поощрять разработку национального законодательства, гарантирующего независимость и плюрализм средств массовой информации.

c) Принять надлежащие меры — не посягая при этом на свободу слова — для борьбы с незаконным и наносящим ущерб контентом в СМИ.

d) Поощрять профессиональных работников средств массовой информации в развитых странах к установлению партнерских отношений и созданию сетей со средствами массовой информации в развивающихся странах, в особенности в области профессиональной подготовки.

e) Поддерживать создание гармоничного и многогранного образа женщины и мужчины в средствах массовой информации.

f) Сокращать существующие на международном уровне и сказывающиеся на СМИ диспропорции, особенно в отношении инфраструктуры, технических ресурсов и развития навыков и умений людей, используя для этой цели все преимущества, которые предоставляют в этом отношении инструменты на базе ИКТ.

g) Поощрять традиционные средства массовой информации к преодолению разрыва в знаниях и содействию распространению культурного контента, особенно в сельских районах.

C10. Этические аспекты информационного общества

25. Информационное общество должно опираться на общепризнанные ценности и заботиться об общем благе, а также предотвращать злоупотребления при использовании ИКТ.

a) Принимать меры для укрепления мира и отстаивания таких основных ценностей, как свобода, равенство, солидарность, терпимость, коллективная ответственность и бережное отношение к природе.

b) Все заинтересованные стороны должны полнее учитывать этический аспект при применении ИКТ.

c) Все участники информационного общества должны заботиться об общем благе, защищать неприкосновенность частной жизни и личных сведений, предпринимать соответствующие действия и принимать установленные законом меры по предотвращению ненадлежащего использования ИКТ, такого как противоправные деяния и прочие действия на почве расизма, расовой дискриминации, ксенофобии и связанных с ними нетерпимости, ненависти, насилия, всех форм жестокого обращения с детьми, включая педофилию и детскую порнографию, а также торговля людьми и их эксплуатация.

d) Привлекать соответствующие заинтересованные стороны, прежде всего ученых, к продолжению исследования этических аспектов ИКТ.

C11. Международное и региональное сотрудничество

26. Международное сотрудничество всех заинтересованных сторон имеет решающее значение для осуществления настоящего Плана действий и должно укрепляться в целях содействия реализации универсального доступа и ликвидации разрыва в цифровых технологиях, в частности путем обеспечения способов реализации.

a) Органы государственного управления развивающихся стран должны повышать относительную степень приоритетности проектов в области ИКТ в запросах в отношении международного сотрудничества и оказания помощи по проектам развития инфраструктуры со стороны развитых стран и международных финансовых организаций.

b) В контексте Глобального договора ООН и с опорой на Декларацию тысячелетия Организации Объединенных Наций создавать и развивать партнерские отношения между государственным и частным секторами, уделяя особое внимание использованию ИКТ в интересах развития.

c) Предложить международным и региональным организациям включать ИКТ в основные направления своих рабочих программ и оказывать поддержку развивающимся странам, находящимся на разных уровнях развития, в составлении и реализации национальных планов действий, направленных на достижение целей, указанных в Декларации принципов и настоящем Плане действий, учитывая при этом значимость региональных инициатив.

D. Повестка дня цифровой солидарности

27. Целью Повестки дня цифровой солидарности является создание условий для мобилизации людских, финансовых и технологических ресурсов, необходимых для

включения всех мужчин и женщин в формирующееся информационное общество. Жизненно важное значение для выполнения этой Повестки дня имеет тесное сотрудничество всех заинтересованных сторон на национальном, региональном и международном уровнях. Для преодоления разрыва в цифровых технологиях нам потребуется с большей эффективностью использовать существующие подходы и механизмы и в полной мере освоить новые подходы и механизмы, с тем чтобы обеспечивать финансирование развития инфраструктуры, оборудования, наращивания потенциала и создания контента, необходимых для участия в информационном обществе.

D1. Приоритеты и стратегии

a) Национальные электронные стратегии должны составлять неотъемлемую часть национальных планов в области развития, включая стратегии сокращения масштабов бедности.

b) ИКТ должны быть полностью включены в основные направления стратегий официальной помощи в целях развития (ОПР) посредством более эффективного обмена информацией и координации с донорами, а также посредством анализа наилучшей практики и уроков, извлеченных из опыта применения ИКТ в программах в области развития, и обмена ими.

D2. Мобилизация ресурсов

a) Все страны и международные организации должны работать над созданием условий, благоприятствующих повышению доступности и эффективной мобилизации ресурсов для финансового развития, как указано в Монтеррейском консенсусе.

b) Развитые страны должны принять конкретные меры для выполнения своих международных обязательств по финансированию развития, включая содержащиеся в Монтеррейском консенсусе, где к тем развитым странам, которые еще этого не сделали, обращен настоятельный призыв принять конкретные меры для достижения целевого уровня ОПР развивающимся странам, составляющего 0,7 процента от их валового национального продукта (ВНП), а также выделения наименее развитым странам 0,15–0,20 процента ВНП развитых стран.

c) Мы приветствуем инициативы в пользу страдающих от непомерного долгового бремени развивающихся стран, направленные на уменьшение непогашенной задолженности, и предлагаем принять дальнейшие национальные и международные меры в этом направлении, в том числе, в соответствующих случаях, аннулировать долги и заключать иные договоренности. Особое внимание следует уделять развитию инициативы в отношении бедных стран с крупной задолженностью. Эти инициативы позволят высвободить больше ресурсов, которые могут использоваться для финансирования проектов в области ИКТ в целях развития.

d) Учитывая потенциал ИКТ для целей развития, мы далее призываем:

i) развивающиеся страны — активизировать свои усилия по привлечению крупных частных национальных и иностранных инвестиций в ИКТ путем создания прозрачного, стабильного, предсказуемого и благоприятного инвестиционного климата;

ii) развитые страны и международные финансовые организации — должным образом реагировать на стратегии и приоритеты ИКТ в целях развития, включить ИКТ в свои рабочие программы и содействовать развивающимся странам и странам с переходной экономикой в разработке и реализации национальных электронных стратегий. На основании приоритетов национальных планов развития и осуществления вышеуказанных обязательств развитые страны должны увеличить предпринимаемые ими усилия по предоставлению большего объема финансовых ресурсов развивающимся странам для применения ИКТ в целях развития;

iii) частный сектор — вносить свой вклад в реализацию настоящей Повестки дня цифровой солидарности.

e) В своих усилиях по преодолению разрыва в цифровых технологиях нам следует содействовать, в рамках нашего сотрудничества в области развития, оказанию технической и финансовой помощи, направленной на наращивание национального и регионального потенциала, передачу технологий на взаимосогласованных условиях, сотрудничество по программам НИОКР и обмен ноу-хау.

f) Следует в полной мере использовать все существующие финансовые механизмы и при этом завершить к концу декабря 2004 года детальный анализ их соответствия задачам по применению ИКТ в целях развития. Этот анализ должен проводиться какой-либо целевой группой, действующей под эгидой Генерального секретаря Организации Объединенных Наций, а его результаты должны быть представлены на рассмотрение в рамках второго этапа настоящей Встречи на высшем уровне. На основе результатов анализа следует рассмотреть вопрос о совершенствовании и обновлении финансовых механизмов, в том числе об эффективности, целесообразности и создании добровольного фонда цифровой солидарности, упомянутого в Декларации принципов.

g) Странам следует рассмотреть вопрос о создании национальных механизмов обеспечения универсального доступа в обслуживаемых в недостаточной степени сельских и городских районах с целью преодоления разрыва в цифровых технологиях.

E. Последующие меры и оценка

28. Следует разработать реалистичную международную систему оценки и определения (как качественного, так и количественного) эффективности, используя сопоставимые статистические показатели и результаты исследований, с тем чтобы вести наблюдение за выполнением задач, достижением целей и контрольных показателей Плана действий, принимая во внимание национальные особенности.

a) В сотрудничестве с каждой заинтересованной страной разработать и ввести сводный индекс показателей развития ИКТ (цифровых возможностей). Его можно было бы публиковать ежегодно или раз в два года в Отчете о развитии ИКТ. В индексе приводились бы статистические данные, а в отчете представлялись аналитические исследования принятой в них политики и результатов ее проведения в зависимости от национальных особенностей, в том числе данные гендерного анализа.

b) Надлежащие показатели и ориентиры, в том числе показатели коллективного доступа, должны отражать величину разрыва в цифровых технологиях как в национальном, так и в международном масштабе и обеспечивать его регулярную оценку, с тем чтобы отслеживать мировые достижения в использовании ИКТ для решения согласованных на международном уровне задач, включая те, которые содержатся в Декларации тысячелетия.

c) Международные и региональные организации должны проводить оценку и на регулярной основе представлять доклады об уровне универсальной доступности ИКТ в различных странах, с тем чтобы обеспечить создание равных возможностей для развития секторов ИКТ в развивающихся странах.

d) Следует разработать учитывающие гендерную специфику показатели по применению ИКТ и потребностям в них, а также определить поддающиеся количественному измерению показатели выполнения с целью оценки воздействия финансируемых проектов в области ИКТ на жизнь женщин и девочек.

e) Подготовить и открыть основанный на материалах, поступивших в качестве вкладов от всех заинтересованных сторон, Web-сайт, посвященный образцам наилучшей практики и успешно проведенным мероприятиям, формат которого должен быть четким, доступным и наглядным, согласно признанным на международном уровне стандартам сетевой доступности. Web-сайт можно было бы периодически обновлять и превратить его в средство постоянного обмена опытом.

f) Всем странам и регионам следует разработать инструменты, необходимые для предоставления статистической информации по вопросам информационного общества, включающей базовые показатели и анализ динамики его ключевых параметров. Приоритет следует отдавать созданию согласованных и сопоставимых на международном уровне систем показателей, принимая во внимание различия в уровнях развития.

F) Готовясь ко второму этапу ВВУИО (Тунис)

29. В соответствии с резолюцией 56/183 Генеральной Ассамблеи и с учетом итогов женевского этапа ВВУИО следует провести в первой половине 2004 года подготовительное собрание с целью анализа тех относящихся к информационному обществу вопросов, которые будут фигурировать в качестве основных в рамках тунисского этапа ВВУИО, и принятия решения относительно структуры процесса подготовки ко второму этапу. Согласно решению, принятому настоящей Встречей на высшем уровне в отношении ее тунисского этапа, на втором этапе ВВУИО необходимо рассмотреть, в частности, следующие вопросы:

a) разработка соответствующих заключительных документов на основании итогов женевского этапа ВВУИО, с целью консолидации процесса построения глобального информационного общества, сокращения разрыва в цифровых технологиях и превращения его в цифровые возможности;

b) последующие меры и реализация Женевского плана действий на национальном, региональном и международном уровнях, в том числе в системе Организации Объединенных Наций, в рамках целостного и согласованного подхода, предусматривающего участие всех соответствующих заинтересованных сторон. Эти действия должны проводиться, в частности, в рамках партнерских отношений между заинтересованными сторонами.

Неофициальный перевод с английского языка

Национальная стратегия обеспечения безопасности киберпространства США

THE WHITE HOUSE WASHINGTON Белый дом **Вашингтон**

Сограждане-американцы,

Способ ведения бизнеса, действия правительства, руководства национальной обороной изменился. Вся эта деятельность опирается сейчас на взаимозависимую сеть инфраструктур информационной технологии, называемую киберпространством. *Национальная стратегия обеспечения безопасности киберпространства* предоставляет структуру для защиты этой необходимой для нашей экономики, безопасности и образа жизни инфраструктуры.

В последние несколько лет связанные с киберпространством угрозы значительно выросли. Политика Соединенных Штатов состоит в защите от наносящего ущерб нарушения работы информационных систем критических инфраструктур и, таким образом, в содействии защите людей, экономики и национальной безопасности США. Мы должны действовать, чтобы уменьшить уязвимости к этим угрозам, прежде чем они могут быть использованы для нанесения ущерба кибернетическим системам, поддерживающим критические инфраструктуры нашей страны, и чтобы гарантировать, что такие нарушения киберпространства будут нечастыми, будут иметь минимальную длительность, с ними можно будет справиться и они будут причинять наименьший возможный ущерб.

Обеспечение безопасности киберпространства представляет собой необычайно трудную стратегическую задачу, требующую скоординированных и сосредоточенных усилий всего нашего общества — федерального правительства, властей штатов, местных властей, частного сектора и всего американского народа. Для привлечения американцев к обеспечению безопасности киберпространства был выпущен проект данной стратегии для общественных отзывов и проведено десять муниципальных встреч по всей стране с целью сбора информации по развитию национальной стратегии. Тысячи людей и многие организации приняли участие в этих муниципальных встречах и представили свои комментарии. Я благодарю всех за их продолжающееся участие в этом процессе.

Краеугольным камнем американской стратегии обеспечения безопасности киберпространства является и останется партнерство государственного и частного секторов. Федеральное правительство призывает к созданию и участию в партнерстве государственного и частного секторов для осуществления этой стратегии. Только совместными действиями мы сможем создать более безопасное будущее киберпространства.

Джордж Буш

Организационное резюме

Критические инфраструктуры нашей страны составляют государственные и частные учреждения следующих секторов: сельскохозяйственного, производства пищевых продуктов, водоснабжения, здравоохранения, служб экстренной помощи, правительства, оборонной промышленной базы, информации и телекоммуникаций, энергетики, транспорта, банковского дела и финансов, химикатов и опасных веществ, почтового сектора и сектора перевозок. Киберпространство представляет собой их «нервную систему», систему контроля нашей страны. Киберпространство составляют сотни тысяч взаимосвязанных компьютеров, серверов, маршрутизаторов-переключателей, волоконно-оптических кабелей, дающих возможность работать нашим критическим инфра-

структурам. Таким образом, безопасное функционирование киберпространства является необходимым для нашей экономики и национальной безопасности.

Данная *Национальная стратегия обеспечения безопасности киберпространства* представляет собой часть наших общих усилий по защите страны. Это неотъемлемый компонент *Национальной стратегии обеспечения национальной безопасности,* который дополняет *Национальная стратегия физической защиты критических инфраструктур и основных активов.* Цель данного документа — привлечь и уполномочить американцев обеспечивать безопасность тех частей киберпространства, которыми они владеют, управляют, контролируют или с которыми взаимодействуют. Обеспечение безопасности киберпространства представляет собой необычайно трудную стратегическую задачу, требующую скоординированных и сосредоточенных усилий всего нашего общества: федерального правительства, властей штатов, местных властей, частного сектора и всего американского народа.

Национальная стратегия обеспечения безопасности киберпространства обрисовывает первоначальную структуру для организационных и первостепенных усилий. Она дает общее направление ведомствам и организациям федерального правительства, играющим свои роли в обеспечении безопасности киберпространства. Она также определяет шаги, которые могут быть предприняты властями штатов и местными властями, частными компаниями и организациями, а также отдельными американцами для улучшения безопасности киберпространства. *Национальная стратегия обеспечения безопасности киберпространства* выдвигает на передний план партнерство государственного и частного секторов. Этот документ обеспечивает структуру для вкладов, которые все мы можем внести для обеспечения безопасности наших частей киберпространства. С течением времени динамика киберпространства потребует внесения корректировок и исправлений в эту Стратегию.

Скорость и анонимность кибернападений затрудняют возможность распознания действий террористов, преступников и государств — задача, часто возникающая только после свершившегося факта, если вообще возникающая. Поэтому *Национальная стратегия обеспечения безопасности киберпространства* помогает уменьшить уязвимости нашей страны к наносящим ущерб нападениям на критические информационные инфраструктуры или поддерживающие их физические активы.

Стратегические цели

В соответствии с *Национальной стратегией обеспечения национальной безопасности* стратегические цели *Национальной стратегии обеспечения безопасности киберпространства* таковы:

- предупреждение кибернападений на критические инфраструктуры США;
- уменьшение национальных уязвимостей к кибернападениям;
- минимизация ущерба и времени восстановления после кибернападений, если таковые произошли.

Угрозы и уязвимости

Наша экономика и национальная безопасность полностью зависят от информационной технологии и информационной инфраструктуры. Центром информационной инфраструктуры, от которой мы зависим, является Интернет, система, первоначально задуманная для того, чтобы дать возможность ученым (которые, как предполагалось, не заинтересованы злоупотреблением сетью) делиться несекретными исследованиями. Тот же самый Интернет сегодня соединяет миллионы компьютерных сетей, заставляя работать большинство важнейших инфраструктур и служб страны. Эти компьютерные сети

также регулируют работу таких физических объектов, как электрические трансформаторы, поезда, насосы трубопроводов, химические резервуары, радары и фондовые рынки, которые существуют вне киберпространства.

Целый ряд злонамеренных действующих лиц может и ведет нападения на наши критические информационные инфраструктуры. Основное беспокойство вызывает угроза организованных кибернападений, способных вызвать наносящий ущерб подрыв критических инфраструктур нашей страны, экономики или национальной безопасности. Необходимый технический опыт для проведения такого нападения должен быть высоким, что частично объясняет отсутствие таких наносящих ущерб нападений до настоящего времени. Однако мы не должны испытывать чрезмерный оптимизм. Были случаи, когда организованные нападающие использовали уязвимости, которые могут указывать на более разрушительные возможности.

Существует неопределенность и в отношении намерения и полных технических возможностей некоторых отслеженных нападений. Необходим улучшенный анализ киберугроз для рассмотрения долгосрочных тенденций, связанных с угрозами и уязвимостями. Известно, что инструментальные средства и методологии нападений становятся широко доступными, а технические возможности и опыт пользователей, склонных к созданию беспорядка или разрушений, возрастают.

В мирное время противники США могут вести шпионаж в правительстве, университетских исследовательских центрах и частных компаниях. Они могут также стремиться к подготовке кибернападений во время конфронтации, составляя план информационных систем США, устанавливая ключевые цели и вплетая в нашу инфраструктуру лазейки и другие средства доступа. В военное время или во время кризиса противники могут стремиться к запугиванию политических деятелей страны путем нападения на критические инфраструктуры и основные экономические функции или разрушения общественного доверия к информационным системам.

Кибернападения на информационные сети Соединенных Штатов могут иметь такие серьезные последствия, как нарушение важнейших операций, потери доходов и интеллектуальной собственности или людские потери. Противостояние таким нападениям требует развития прочных возможностей там, где их не существует сегодня, если мы собираемся уменьшить уязвимости и помешать тем, кто имеет намерение и возможности причинить ущерб нашим критическим инфраструктурам.

Роль государства в обеспечении безопасности киберпространства

В целом частный сектор лучше оснащен и структурирован для реагирования на развивающиеся киберугрозы. Однако существуют определенные случаи, где реакция федерального правительства является наиболее уместной и оправданной. С внутренней стороны, обеспечение непрерывности действий правительства требует обеспечения надежности его собственных кибернетических инфраструктур и активов, необходимых для поддержки его важнейших задач и служб. С внешней стороны, роль государства в обеспечении безопасности киберпространства оправдана в тех случаях, когда высокие операционные расходы или юридические барьеры приводят к существенным проблемам координации; в случаях, когда государство действует в отсутствии сил частного сектора; для разрешения побудительных проблем, ведущих к недостаточному обеспечению совместно используемых критических ресурсов, а также для повышения осознания безопасности.

Партнерство государственного и частного секторов представляет собой ключевой компонент нашей *Стратегии обеспечения безопасности киберпространства*. Это так по нескольким причинам. Партнерство государственного и частного секторов может успешно противостоять проблемам координации. Оно может значительно улучшить ин-

формационный обмен и сотрудничество. Партнерство государственного и частного секторов может принимать различные формы и будет направлено на повышение осознания, обучение, технологические усовершенствования, исправление уязвимостей и восстановительные операции.

Федеральная роль в этих и других случаях оправдана только тогда, когда выгоды вмешательства перевешивают соответствующие расходы. Этот стандарт особенно важен в тех случаях, когда существуют жизнеспособные решения частного сектора для рассмотрения любых потенциальных угроз или уязвимостей. В каждом случае следует рассматривать общие расходы и влияния данного правительственного решения в сравнении с другими альтернативными действиями и в сравнении с отсутствием действий, принимая в расчет любые существующие или будущие решения частного сектора.

Федеральные действия по обеспечению безопасности киберпространства оправданы для целей: судебного преследования и установления источника нападения, защиты сетей и систем, имеющих критическое значение для национальной безопасности, указаний и предупреждений, а также для защиты от организованных нападений, способных нанести ущерб экономике. Федеральные действия должны также поддерживать исследования и развитие технологии, которые позволят частному сектору лучше защищать находящиеся в частном владении части критической инфраструктуры США.

Министерство национальной (внутренней) безопасности и безопасность киберпространства

22 ноября 2002 года президент Буш подписал законопроект по созданию Министерства национальной (внутренней) безопасности Это новое ведомство министерского уровня объединит 22 федеральные организации для общей цели улучшения нашей национальной безопасности. У министра будут важные обязанности по обеспечению безопасности киберпространства. Эти обязанности включают:

- разработку всестороннего национального плана обеспечения безопасности основных ресурсов и критической инфраструктуры США;
- обеспечение кризисного управления в ответ на нападения на критические информационные системы;
- предоставление технической помощи частному сектору и другим государственным организациям в отношении планов экстренного восстановления в случае повреждения критических информационных систем;
- согласование с другими организациями федерального правительства вопросов предоставления определенной предупреждающей информации и рекомендаций по соответствующим защитным мерам и контрмерам для организаций на уровне штата, местных и негосударственных организаций, включая частный сектор, академические круги и общественность;
- проведение и финансирование вместе с другими организациями исследований и разработок, ведущих к выработке нового научного понимания и технологий в поддержку национальной безопасности.

В соответствии с этими обязанностями министерство станет федеральным центром мастерства в обеспечении безопасности киберпространств и фокальной точкой для связи федерального правительства с организациями на уровне штата, местными и негосударственными организациями, включая частный сектор, академические круги и общественность.

Важнейшие приоритеты для безопасности киберпространства

Национальная стратегия обеспечения безопасности киберпространства формулирует пять национальных приоритетов, которые включают:

I. Национальную систему реагирования на инциденты безопасности киберпространства;

II. Национальную программу уменьшения уязвимостей и угроз безопасности киберпространства;

III. Национальную программу обучения и повышения осознания безопасности киберпространства;

IV. Обеспечение безопасности государственного киберпространства;

V. Национальную безопасность и международное сотрудничество по обеспечению безопасности киберпространства.

Первый приоритет сосредотачивается на улучшении реагирования на инциденты в киберпространстве и уменьшении потенциального ущерба от таких событий. Целью второго, третьего и четвертого приоритетов является уменьшение угроз кибернападений и уязвимостей к ним. Пятый приоритет относится к предотвращению кибернападений, которые могут повлиять на активы национальной безопасности, и улучшению международного менеджмента и реагирования на такие нападения.

Приоритет I: Национальная система реагирования на инциденты безопасности киберпространства

Быстрое определение, обмен информацией и исправление часто могут уменьшать ущерб, причиненный злонамеренной деятельностью в киберпространстве. Чтобы эти мероприятия были эффективными на национальном уровне, Соединенным Штатам необходимо партнерство государства и индустрии для проведения анализа, выпуска предупреждений и координации усилий по реагированию. В этом процессе необходима защита неприкосновенности частной жизни и гражданских прав. Поскольку никакой план по обеспечению безопасности киберпространства не может быть неприступным для спланированного и интеллектуального нападения, информационные системы должны уметь работать при таком нападении и обладать способностью быстрого и полного восстановления операций.

Национальная стратегия обеспечения безопасности киберпространства определяет восемь основных мероприятий и инициатив для реагирования на инциденты безопасности киберпространства:

1. Создание государственно-частной архитектуры для реагирования на кибернетические инциденты национального уровня;

2. Обеспечение разработки тактического и стратегического анализа кибернападений и оценки уязвимостей;

3. Стимулирование развития возможностей частного сектора для совместного синоптического обзора состояния киберпространства;

4. Расширение сети кибернетической информации и предупреждений для поддержки роли DHS в координации кризисного управления для обеспечения безопасности киберпространства;

5. Улучшение национального менеджмента инцидентов;

6. Координация процессов добровольного участия в разработке национальных планов непрерывности действий государственного и частного секторов и действий в чрезвычайных обстоятельствах;

7. Применение планов непрерывности обеспечения безопасности киберпространства для федеральных систем;

8. Улучшение и совершенствование совместного использования информации, касающейся кибернападений, угроз и уязвимостей, государственным и частным секторами.

Приоритет II: Национальная программа уменьшения уязвимостей и угроз безопасности киберпространства

Воспользовавшись уязвимостями в наших кибернетических системах, организованное нападение может подвергнуть риску безопасность критических инфраструктур нашей страны. Уязвимости, представляющие наибольшую угрозу для киберпространства, встречаются в информационных активах самих предприятий критической инфраструктуры и во внешних поддерживающих структурах, таких как механизмы Интернета. Менее защищенные сайты взаимосвязанной сетевой системы сетей также представляют собой потенциально важные незащищенные места для кибернападений. Уязвимости появляются в результате слабостей технологии и неправильного внедрения технологических продуктов и их контроля.

Национальная стратегия обеспечения безопасности киберпространства определяет восемь основных мероприятий и инициатив для уменьшения угроз и соответствующих уязвимостей:

1. Улучшение возможностей деятельности правоохранительных органов по предупреждению и судебному преследованию кибернападений;
2. Создание процесса национальной оценки уязвимостей для лучшего понимания потенциальных последствий наличия угроз и уязвимостей;
3. Защита механизмов Интернета путем улучшения протоколов и маршрутизации;
4. Стимулирование использования доверенных систем цифрового управления/управления в супервизорном режиме и систем сбора данных;
5. Уменьшение и устранение уязвимостей программного обеспечения;
6. Осознание взаимозависимости инфраструктуры и улучшение физической безопасности кибернетических систем и телекоммуникаций;
7. Первостепенное внимание вопросам разработки и исследований в сфере федеральной кибербезопасности;
8. Оценка и обеспечение безопасности появляющихся систем.

Приоритет III: Национальная программа обучения и повышения осознания безопасности киберпространства

Многие уязвимости киберпространства существуют из-за отсутствия осознания безопасности киберпространства со стороны пользователей компьютеров, системных администраторов, разработчиков технологии, должностных лиц, отвечающих за приобретение, аудиторов, управляющих по информации (СЮ), высшего руководства и правления корпораций. Такие связанные с осознанием уязвимости представляют серьезный риск для критических инфраструктур независимо от того, существуют ли они в самой инфраструктуре. Недостаток обученного персонала и отсутствие широко признанных, многоуровневых программ аттестации для специалистов в сфере безопасности киберпространства осложняют задачу работы с уязвимостями киберпространства.

Национальная стратегия обеспечения безопасности киберпространства определяет четыре основных мероприятия и инициативы для повышения осознания, обучения и образования:

1. Создание всесторонней национальной системы повышения осознания, чтобы уполномочить всех американцев — деловые круги, рабочую силу и обычное население — обеспечивать безопасность своих частей киберпространства;
2. Стимулирование адекватных программ обучения и образования для поддержки потребностей безопасности киберпространства страны;

3. Увеличение эффективности существующих федеральных программ обучения в сфере безопасности киберпространства;

4. Стимулирование поддержки частного сектора для хорошо согласованных и широко признанных профессиональных аттестаций в сфере обеспечения безопасности киберпространства.

Приоритет IV: Обеспечение безопасности государственного киберпространства

Хотя власти управляют только меньшей частью компьютерных систем критических инфраструктур США, власти на всех уровнях осуществляют важнейшие услуги в сельскохозяйственном секторе, секторе производства пищевых продуктов, водоснабжения, здравоохранения, служб экстренной помощи, обороны, социального обеспечения, информации и телекоммуникаций, энергетики, транспорта, банковского дела и финансов, химикатов, перевозок и почтового сектора, поставка которых зависит от киберпространства. Власти могут подавать пример в обеспечении безопасности киберпространства, включая стимулирование рынка более безопасных технологий посредством своих закупок.

Национальная стратегия обеспечения безопасности киберпространства определяет пять основных мероприятий и инициатив для обеспечения безопасности государственного киберпространства:

1. Постоянная оценка уязвимостей и угроз федеральным кибернетическим системам;

2. Аутентификация и обслуживание уполномоченных пользователей федеральных кибернетических систем;

3. Обеспечение безопасности федеральных беспроводных локальных сетей;

4. Улучшение безопасности государственных приобретений и привлечения внешних ресурсов;

5. Побуждение властей штатов и местных властей к рассмотрению вопроса создания программ по безопасности информационной технологии и участия в работе центров обмена и анализа информации с аналогичными властями.

Приоритет V: Национальная безопасность и международное сотрудничество по обеспечению безопасности киберпространства

Киберпространство Америки связывает США с остальным миром. Сетевая система сетей охватывает всю планету, позволяя злонамеренным действующим лицам на одном континенте воздействовать на системы, расположенные на расстоянии тысяч миль.

Кибернападения пересекают границы со скоростью света, и распознание источника злонамеренной деятельности представляет собой трудную задачу. Соединенные Штаты должны быть способны охранять и защищать свои критические системы и сети. Для этого необходима система международного сотрудничества, помогающая облегчить совместное использование информации, уменьшить уязвимости и удержать злонамеренных действующих лиц.

Национальная стратегия обеспечения безопасности киберпространства определяет шесть основных мероприятий и инициатив для укрепления национальной безопасности США и международного сотрудничества:

1. Усиление связанных с киберпространством действий контрразведки;

2. Улучшение возможностей определения источника нападения и реагирования;

3. Улучшение координации в сфере национальной безопасности США для реагирования на кибернападения;

4. Работа с промышленными и международными организациями для облегчения диалога и содействия партнерству с международными государственными и частными секторами, сосредоточенного на защите информационных структур и стимулировании развития глобальной «культуры безопасности»;

5. Стимулирование создания национальных и международных сетей наблюдения/предупреждения для обнаружения и предотвращения кибернападений;

6. Побуждение других государств присоединиться к Совету европейской конвенции по киберпреступлениям или обеспечить, чтобы их законы и процедуры были, по крайней мере такими же обстоятельными.

Национальные усилия

Защита широко рассредоточенных активов киберпространства требует усилий многих американцев. Федеральное правительство в одиночку не может обеспечить достаточную защиту киберпространства США. Наши традиции федерализма и ограничения власти требуют, чтобы организации, не относящиеся к федеральному правительству, взяли на себя инициативу во многих из таких усилий. Каждый американец, который может внести вклад в обеспечение безопасности части киберпространства, поощряется к этому. Федеральное правительство призывает к созданию и участию в партнерстве государственного и частного секторов для повышения осознания безопасности киберпространства, обучения персонала, стимулирования рыночных сил, улучшения технологии, идентификации и исправления уязвимостей, обмена информацией и планирования восстановительных операций.

Люди и организации на всей территории США уже предприняли определенные шаги для улучшения безопасности киберпространства. 18 сентября 2002 года многие организации частного сектора опубликовали планы и стратегии обеспечения безопасности своих инфраструктур. Партнерство ради безопасности критической инфраструктуры сыграло уникальную роль в содействии вкладу частного сектора в данную Стратегию. Информацию, поступающую от секторов критической инфраструктуры, можно найти на сайте http://www.pcis.org. (Эти документы не подлежат правительственному утверждению.)

Эти обстоятельные планы инфраструктуры описывают стратегические инициативы различных секторов, включая следующие:

- банковского дела и финансов;
- страхования;
- химии;
- нефти и газа;
- электроэнергии;
- правоприменения.

МИНИСТЕРСТВО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ РОССИЙСКОЙ ФЕДЕРАЦИИ

НОРМАТИВНЫЕ ДОКУМЕНТЫ

Проект

Государственная программа "Создание в Российской Федерации технопарков в сфере информационных технологий"

Проект

Государственная программа «Создание в Российской Федерации технопарков в сфере информационных технологий»

1. Обоснование соответствия решаемой проблемы задачам социально-экономического развития Российской Федерации

Развитие и распространение информационно-коммуникационных технологий является важным фактором мирового экономического роста. Их широкое применение имеет решающее значение для повышения производительности и оптимизации деятельности предприятий и организаций практически всех отраслей экономики, а также модернизации и повышения эффективности основных институтов государственного управления.

Отрасль информационных технологий — субъекты экономической деятельности, участвующие в создании, развитии и распространении информационных технологий.

К отрасли информационных технологий относятся: разработка программ для электронных вычислительных машин и баз данных и продажа их в виде отдельных экземпляров без передачи имущественных прав; разработка программ для электронных вычислительных машин и баз данных и передача исключительных прав либо неисключительных прав на них на основе лицензионного (авторского) договора о передаче прав; предоставление услуг, связанных с проектированием, разработкой, внедрением, поддержкой и обслуживанием программного обеспечения и компьютерного оборудования и программного обеспечения, а также производство оборудования для создания и эксплуатации перечисленного.

Спрос на информационно-коммуникационные технологии неуклонно растет, а их возможности стремительно расширяются. Отрасль информационно-коммуникационных технологий стала локомотивом развития мировой экономики. Ее доля в структуре ВВП ведущих стран мира увеличивается и составляет в настоящее время от 5 до 20 процентов, а общемировые темпы роста на уровне 8-9 процентов в год значительно превышают темпы развития отраслей традиционной «индустриальной» экономики — металлургии, машиностроения, топливно-энергетического комплекса. Информационно-коммуникационные технологии заняли одно из ведущих мест в структуре международной торговли, их доля за последние десятилетия стремительно выросла и в настоящее время превышает объемы международной торговли вооружением и военной техникой.

Рост отрасли информационно-коммуникационных технологий в меньшей степени зависит от традиционных факторов производства: размеров существующей производственной инфраструктуры и объемов имеющихся природных ресурсов.

Ключевым фактором ее успешного развития является качество человеческого капитала и его интеллектуальный потенциал. Это создает широкие возможности для успешной интеграции в мировую экономику многих развивающихся стран.

Высокие темпы развития отрасли сохранятся и в ближайшие десятилетия, поддерживаемые многообещающими перспективами новых разработок, близкими к практической реализации, и дальнейшим ростом спроса а продукцию и услуги в сфере информационно-коммуникационных технологий.

Российский рынок информационно-коммуникационных технологий на протяжении последних десяти лет демонстрирует опережающие по отношению к экономике страны в целом и одни из самых высоких в мире темпы роста в среднем на уровне 20 процентов в год. Это во многом обусловлено низким первоначальным уровнем их использования в социально-экономической сфере и высоким спросом на них. **Несмотря на значительные темпы роста российского рынка информационно-коммуникационных технологий, отечественное производство конкурентоспособной продукции в этой сфере только формируется и по уровню своего развития значительно отстает не только от западных стран, но и некоторых стран Восточной Европы и Азии.**

Из-за отсутствия собственного производства компьютерного оборудования и базового программного обеспечения, соответствующего мировому уровню, в настоящее время основная доля российских предприятий в сфере информационно-коммуникационных технологий не создает продукции с высокой добавленной стоимостью, а поставляет на российский рынок продукцию зарубежных производителей.

В мировом масштабе рынок компьютерного оборудования и комплектующих уже сложился и характеризуется высоким уровнем конкуренции, низким уровнем прибыльности и концентрацией основного производства в странах Юго-Восточной Азии. Как показывает мировой опыт, по мере формирования и развития капиталоемкой инфраструктуры промышленного производства компьютерного оборудования и комплектующих в странах с дешевой рабочей силой основной вектор конкуренции в отрасли информационно-коммуникационных технологий переместился в сектор перспективных разработок и создания программного обеспечения. Данное производство характеризуется высокой мобильностью, при наличии необходимых каналов связи оно может размещаться в любой географической точке страны, его организация не требует значительных инвестиций в создание производственной инфраструктуры. Ключевым фактором успеха является квалификация специалистов, их интеллектуально-творческий потенциал.

Для успешной конкуренции в этой сфере в России имеется целый ряд серьезных предпосылок. Разработка новой продукции в сфере информационно-коммуникационных технологий, особенно программного обеспечения, в целом соответствует основному профилю российского высшего образования, ориентированному, в первую очередь, на обучение естественным и точным наукам. В России создана эффективная система воспроизводства квалифицированных инженеров и специалистов в сфере прикладной математики, вычислительной техники и программирования, конкурентоспособных на мировом рынке труда. Студенты российских вузов неоднократно выигрывали и становились призерами всемирных олимпиад по программированию. Несмотря на то, что при обучении традиционно мало внимания уделяется изучению иностранных языков и классических управленческих дисциплин, специалисты в сфере информационно-коммуникационных технологий пользуются высоким спросом за рубежом и составляют основную долю российских специалистов, успешно работающих в иностранных компаниях.

Потенциал российских предприятий в сфере разработки программного обеспечения также подтверждается многочисленными примерами выпуска конкурентоспособных на мировом рынке программных продуктов, однако пока это производство развивается в основном в нише узкоспециализированного программного обеспечения, не ориентировано на широкий потребительский рынок и не носит массового характера. Некоторые российские предприятия также имеют опыт успешного выполнения уникальных масштабных проектов в сфере разработки программного обеспечения по заказу для крупных зарубежных корпораций, однако эти примеры пока носят единичный характер и объемы этих работ невелики по сравнению с основными странами-конкурентами. Основное производство сконцентрировано в Москве и Санкт-Петербурге. В других российских регионах отсутствует необходимая современная инфраструктура поддержки развития интеллектуального ориентированного на экспорт производства в сфере информационно-коммуникационных технологий, отвечающая международным стандартам. Это приводит к тому, что отечественные специалисты в сфере информационно-коммуникационных технологий, выпускаемые российскими вузами, продолжают уезжать из страны из-за отсутствия достаточного количества рабочих мест с конкурентоспособной оплатой труда по месту их проживания. Русскоговорящие квалифицированные специалисты в сфере разработки программного обеспечения из стран ближнего зарубежья с более низкой оплатой труда, которые могли бы стать важным ресурсом развития отечественной отрасли, также предпочитают России развитые страны из-за дополнительных ограничений существующего миграционного законодательства. Развитие отечественной отрасли ограничивает также недоступность финансовых ресурсов и отсутствие механизмов венчурного финансирования перспективных проектов. Несоответствие системы профессиональной подготовки специалистов в сфере информационно-коммуникационных технологий ведущим международным стандартам приводит к дефициту управленческих кадров необходимой квалификации.

Развитие российских предприятий также сдерживается существующими административными барьерами. Существующий порядок таможенного оформления экспорта продукции в сфере информационно-коммуникационных технологий приводит к задержкам в оформлении экспорта и росту административных расходов компаний, стимулируя увод экспортных операций в сфере информационно-коммуникационных технологий за рубеж, например, через открытие офисов в другой стране. Применяемые органами государственной власти механизмы защиты информации также давно перестали быть действенными и создают при экспорте для предприятий отрасли искусственные бюрократические барьеры. Так, экспортные операции в значительной степени усложнены необходимостью получения для каждой сделки сертификатов и лицензий ФАПРИД.

Специфика экспорта программного обеспечения и другой продукции и услуг в сфере информационно-коммуникационных технологий не описана в законодательстве, что осложняет подтверждение факта экспорта программного обеспечения и ИКТ-услуг по каждой отдельной сделке для возврата налога на добавленную стоимость. Все это приводит к тому, что большая часть экспортных операций осуществляется на основе создания зарубежных представительств, филиалов и дочерних компаний, что ведет к потере доходов бюджета. Широкое использование подобных схем затрудняет возможность получения компаниями кредитов и венчурного финансирования, а также осложняет поиск партнеров в России и за рубежом.

Важным вопросом фискального регулирования для предприятий отрасли информационно-коммуникационных технологий является налогообложение расходов по оплате труда. Доля этих расходов в себестоимости производства компаний отрасли

составляет от 60 до 70 процентов. Применение действующих ставок единого социального налога является одним из факторов снижения эффективности конкуренции компаний отечественной отрасли информационно-коммуникационных технологий на мировом рынке. На практике это приводит к переводу центров капитализации российских компаний в страны с более благоприятным налоговым режимом.

Некоторые ведущие технологические зарубежные компании, имеющие успешный опыт работы в России и осознавшие преимущества российских специалистов в сфере информационно-коммуникационных технологий, создают на территории страны собственные центры исследований и перспективных разработок. Однако общий объем иностранных инвестиций в отрасль остается крайне низким из-за отсутствия действенных и эффективных механизмов защиты прав интеллектуальной собственности и специальных мер налогового стимулирования инвестиционной активности в этой сфере.

2. Обоснование целесообразности решения проблемы программным методом

Как показывает мировой опыт, превращение национальной отрасли информационно-коммуникационных технологий в одну их движущих сил экономического роста и модернизации страны в короткие сроки возможно только в случае обеспечения целенаправленной государственной поддержки ее развития. При этом государственная политика должна быть ориентирована в приоритетном порядке на поддержку развития отечественного производства конкурентоспособной на мировом рынке продукции, в том числе имеющей высокий экспортный потенциал.

Достижение показателей развития отрасли информационно-коммуникационных технологий к 2010 году, сопоставимых с показателями ведущих постиндустриальных стран, требует ускоренного развития отечественной отрасли информационно-коммуникационных технологий на уровне 40-45 процентов в среднем в год. Обеспечение таких темпов роста возможно при условии проведения скоординированной государственной политики, направленной на устранение административных барьеров, создание условий для развития и повышения конкурентоспособности российских предприятий в сфере информационно-коммуникационных технологий и продвижение их продукции и услуг на мировой рынок. Успешное проведение необходимых преобразований, затрагивающих многие сферы социально-экономического развития страны, как показывает мировой опыт, не ограничивается изменением и совершенствованием нормативно-правовой базы, но и требует со стороны государства соответствующих расходов на создание необходимой инфраструктуры технопарков и среды для эффективного развития предприятий в сфере информационно-коммуникационных технологий, поддержку перспективных исследований и разработок, а также совершенствование системы образования.

Эффективная координация соответствующих бюджетных расходов возможна только в случае принятия на государственном уровне соответствующей программы, определяющей цели, ожидаемые результаты и ключевые показатели развития отрасли.

Основаниями для выбора программного метода решения являются: необходимость жесткого централизованного планирования проводимых преобразований на всех уровнях; необходимость координации, контроля и оперативной корректировки хода их реализации из единого центра; необходимость эффективного управления и контроля за использованием ресурсов, направляемых на осуществление мероприятий.

3. Характеристика и прогноз развития проблемной ситуации без использования программного метода

Сохранение существующей ситуации в ближайшее время приведет к невозможности эффективного использования имеющегося интеллектуально-творческого по-

тенциала страны, продолжению «утечки мозгов», увеличению технологического отставания России, сохранению высокой зависимости экономики страны от сырьевого сектора и импорта высокотехнологичной продукции.

Если не принять соответствующие меры по обеспечению государственной поддержки отечественной отрасли информационно-коммуникационных технологий, направленные на создание дополнительных стимулов для ее ускоренного развития, уже начиная с 2007 года, по мере насыщения российского рынка зарубежной продукцией произойдет замедление темпов роста его основных сегментов до уровня 10 — 12 процентов в год. Доля российской отрасли информационно-коммуникационных технологий не претерпит значительных изменений как в структуре российского экспорта, так и в общем объеме мирового рынка. Сохранение позиции нетто-импортера информационно-коммуникационных технологий и услуг, не использование окна экспортных возможностей, предоставляемого прогнозируемым на период до 2010 года ростом рынка международного аутсорсинга в сфере информационно-коммуникационных технологий до 140 миллиардов долларов США. Консервация отставания России по уровню использования информационно-коммуникационных технологий от стран 2 группы по классификации ОЭСР, сохранение обеспечивающей роли отрасли информационно-коммуникационных технологий в национальной экономике. Снижение конкурентоспособности и как следствие экспортного потенциала базовых отраслей российской экономики и выход стратегических инвесторов из российских компаний. Постепенное перетекание интеллектуальных ресурсов в наиболее развитые страны и их концентрация в корпорациях «новой экономики» и государствах постиндустриального типа.

4. Возможные варианты решения проблемы, оценка их преимуществ и недостатков

Как показывает мировой опыт, государственная поддержка развития национального производства в сфере информационно-коммуникационных технологий может быть направлена на решение следующих приоритетных задач:

развитие собственного промышленного производства в сфере информационных и коммуникационных технологий, ориентированного на удовлетворение внутреннего спроса, включая импортозамещение;

развитие перспективных научных разработок, производства программных продуктов и предоставления услуг в этой сфере, ориентированного, прежде всего на мировой рынок и потребителей за рубежом.

Развитие собственного производства, ориентированного на внутренний спрос, телекоммуникационного и компьютерного оборудования существенно затруднено из-за отсутствия значительных инвестиций, высокой конкуренции со стороны ведущих западных компаний и низкой стоимости продукции, производимой в Юго-Восточной Азии. Как показал опыт стран Латинской Америки, в частности Бразилии, политика протекционизма требует от государства значительных бюджетных затрат на стимулирование развития компьютерных технологий на протяжении продолжительного периода, так как в отсутствие конкуренции со стороны иностранных производителей национальные компании не имеют стимулов к постоянному совершенствованию продукции и созданию новых товаров и услуг.

Наиболее перспективным направлением развития российского сектора информационно-коммуникационных технологий может стать разработка новых информационных технологий, создание программного обеспечения, в том числе в интересах иностранных компаний.

Ключевым направлением обеспечения государственной поддержки в рамках развития данного направления является создание специализированных технологических парков, что позволит обеспечить территориальную концентрацию фи-

нансовых и интеллектуальных ресурсов для организации производства информационных технологий и услуг. Такая концентрация позволяет снизить издержки на использование инфраструктуры, получить доступ к передовым знаниям и опыту, обеспечить эффективное привлечение кадров и занятость достаточно большого количества специалистов, а также применять методы финансового (налогового и таможенного) стимулирования.

Создание технопарков позволит также решить задачу привлечения ведущих мировых компаний для открытия ими в России исследовательских центров, центров перспективных разработок, промышленных производств, что позволит использовать финансовые, промышленные и управленческие ресурсы международных компаний, создать в стране новые высокооплачиваемые рабочие места и развивать инфраструктуру, а также способствовать приобретению российскими специалистами передового опыта управления проектами в сфере информационно-коммуникационных технологий. Примером такого взаимовыгодного сотрудничества является открытие в России центров разработки и исследований таких лидеров, как «Интел», «Моторола», «Боинг», «Сан Майкросистемс» и других.

5. Цели и задачи Программы

Целями Программы являются: развитие отечественного производства в сфере информационно-коммуникационных технологий, обеспечение его конкурентоспособности и лидирующей роли на мировом рынке, увеличение доли продукции и услуг в сфере информационно-коммуникационных технологий в общей структуре российского экспорта;

повышение инвестиционной привлекательности отрасли, увеличение объемов иностранных инвестиций, направляемых в российские предприятия в сфере информационно-коммуникационных технологий;

превращение российской отрасли информационно-коммуникационных технологий в одну из основных движущих сил экономического роста страны, увеличение ее доли в структуре ВВП страны;

обеспечение высокого уровня инновационности и конкуренции в российской отрасли информационных технологий, развитие малого предпринимательства;

обеспечение эффективного воспроизводства и использования интеллектуально-творческого потенциала страны в сфере информационно-коммуникационных технологий, увеличение доли выпускаемых вузами специалистов соответствующих международным требованиям в этой области, создание новых рабочих мест, увеличение занятости населения в отрасли информационно-коммуникационных технологий и предотвращение дальнейшей «утечки мозгов» за рубеж.

Для достижения этих целей необходимо решить следующие задачи:

устранить административные барьеры для развития российских предприятий и их выхода на мировой рынок;

создать специализированные технопарки в сфере информационно-коммуникационных технологий;

обеспечить совершенствование системы профессиональной подготовки специалистов в сфере информационных технологии в соответствии с современными международными стандартами;

обеспечить поддержку выхода российских предприятий, выпускающих продукцию с высоким экспортным потенциалом, на мировой рынок.

6. Целевые индикаторы и показатели результативности реализации Программы

Наименование показателей	*2006*	*2007*	*2008*	*2009*	*2010*
Доля сектора ИКТ в структуре ВВП	6,2%	7,3%	8,1%	8,9%	0.1
Доля продукции и услуг ИКТ в общей структуре экспорта Российский Федерации	1,7%	2,6%	3,4%	4,2%	0.05
Доля экспорта в объеме сектора ИКТ	0.18	0.21	0.27	0.33	0.4
Доля иностранных инвестиций в структуре инвестиций в российские предприятия ИКТ	0.1	0.12	0.15	0.2	0.28
Доля специалистов в сфере ИКТ в общем объеме ежегодно выпускаемых высшими и средними специальными учебными заведениями специалистов	1,9%	2,0%	2,3%	2,6%	2,9%
Доля специалистов в сфере ИКТ в структуре общей занятости населения	2,2%	2,9%	3,8%	4,5%	0.05
Количество созданных специализированных технопарков в сфере информационных технологий	-	2	3	4	5

7. Основные направления реализации Программы

7.1 Устранение административных барьеров для развития российских предприятий в сфере информационно-коммуникационных технологий и продвижения их продукции на мировой рынок

Требуется внесение изменений в Налоговый кодекс Российской Федерации и Таможенный кодекс Российской Федерации, направленных на стимулирование развития отрасли информационных технологий и повышение ее конкурентоспособности.

Устранение барьеров в фискальном и административном регулировании будет способствовать легализации взаимоотношений с иностранными заказчиками, повышению прозрачности деятельности российских предприятий отрасли информационно-коммуникационных технологий и увеличению собираемости налогов.

Также вне рамок настоящей программы требуется разработка иных мер, направленных на устранение административных барьеров (например: в части упрощения процедуры въезда и получения гражданства специалистов из стран СНГ).

7.2 Создание специализированных технопарков в сфере информационных технологий

Ключевым направлением государственной поддержки развития отечественной отрасли информационно-коммуникационных технологий во многих странах стало создание специализированных технопарков в сфере информационных технологий в целях увеличения объемов производств для удовлетворения растущего внутреннего и внешнего спроса на ИТ продукцию при минимизации их непроизводственных расходов. Именно на предприятия, размещаемые в технопарках, приходится основная доля экспорта в сфере информационно-коммуникационных технологий в таких странах, как Индия, Ирландия, Китай и Израиль.

Целью создания технопарков является формирование доступной для предприятий отрасли инфраструктуры, необходимой для развития производства конкурен-

тоспособной продукции в сфере информационно-коммуникационных технологий с высокой добавленной стоимостью.

Технопарки имеют высокоразвитую и отвечающую современным стандартам инфраструктуру, включая жилье, объекты коммунальной и социальной сферы и коммерческую недвижимость. Технопарки предоставляют предприятиям в сфере информационно-коммуникационных технологий эту инфраструктуру для организации рабочих мест сотрудников на экономически эффективных условиях, что позволяет им сокращать собственные издержки и улучшить финансовые показатели деятельности. Технопарки также обеспечивают предоставление набора необходимых услуг для сопровождения деятельности размещаемых на их территории предприятий, что позволяет последним получить значительную экономию расходов и сконцентрироваться на своей основной деятельности. Так, например, технопарк может оказывать для размещаемых на его территории предприятий юридические, финансовые, информационно-технологические, маркетинговые и другие услуги, которые за счет эффекта масштаба будут предоставляться на привлекательных для малых и средних предприятий условиях.

Технопарк может также выступать юридической оболочкой для технологических коллективов, не нуждающихся в самостоятельном юридическом лице.

Технопарки предполагают наличие (или строительство) в рамках определенной территории офисных зданий и производственных помещений, а также необходимой жилищно-коммунальной, транспортной и телекоммуникационной инфраструктуры для создания предприятиям в сфере информационно-коммуникационных технологий необходимых производственных условий. Практика организации управления технопарками в развитых странах показывает, что наиболее эффективным механизмом управления является передача соответствующих функций уполномоченной организации.

Традиционно технопарки создаются при непосредственном участии профильных университетов и государственных научных институтов. Это сотрудничество является взаимовыгодным и необходимо для успешного развития технопарков. Университеты являются основным источником притока в технопарки новых квалифицированных специалистов, выступают инициатором, заказчиком или соисполнителем проводимых исследований и перспективных разработок. Наличие тесных отношений с университетами также позволяет обеспечить необходимый уровень информированности работающих в технопарке специалистов о новых тенденциях в развитии технологий и повышение их квалификации без отрыва от основного производства. На предприятиях, размещаемых на территории технопарков, также организуется прохождение студентами практики, что позволяет им успешно сочетать полученные теоретические знания и реальный практический опыт работы.

Технопарки могут размещаться, в том числе на территориях, обладающих статусом особых экономических зон. В отрасли существует широкий интерес к созданию российских технопарков нового поколения, что во многом обусловлено в целом успешной историей развития в СССР таких коллективных инновационных структур, как закрытые территориальные административные образования, и в последующей «наукоградов».

В настоящее время рядом крупных российских предприятий в сфере информационно-коммуникационных технологий в инициативном порядке реализуются проекты по созданию специализированных технопарков без государственной поддержки. В настоящее время в Российской территории функционируют около 40 разнопрофильных технопарков. Специализированных технопарков в сфере информационных технологий не существует.

В рамках реализации предлагаемой Программы технопарки планируется создавать на базе уже сложившихся в Российской Федерации профильных центров

развития индустрии, расположенных в регионах, определенных в соответствующем поручении Президента Российской Федерации. Критерием отбора регионов являлись: наличие квалифицированных кадров и центров их подготовки, успешно развивающихся российских и зарубежных технологических компаний, имеющих потенциал роста, а также существующего материально-технического задела для построения соответствующей инфраструктуры.

Предполагается, что среднее количество рабочих мест в каждом создаваемом технопарке может составить от 10 до 20 тысяч. Создание технопарков требует значительных финансовых средств, направляемых, в основном, на строительство и реконструкцию объектов недвижимости и инженерных коммуникаций.

Основным направлением поддержки создания технопарков из средств федерального бюджета является софинансирование создания их основной инфраструктуры. Региональные и муниципальные власти в рамках программы обеспечивают выделение земельных участков для строительства технопарков, софинансирование создания инфраструктуры технопарка.

Финансирование строительства необходимых офисных и жилых зданий и помещений может осуществляться за счет средств частных инвесторов.

Предполагается, что до конца 2010 года будет создано 5 технопарков. В дальнейшем решение о создании технопарка, в том числе за счет средств федерального бюджета, должно приниматься на федеральном уровне на конкурсной основе по результатам анализа заявок регионов, содержащих данные о предлагаемых для строительства земельных участках, бюджетном софинансировании и привлеченных инвестициях.

Важнейшим фактором обеспечения конкурентоспособности отрасли информационно-коммуникационных технологий является качество профессионального образования и квалификация трудовых ресурсов. В этой сфере «человеческий фактор» является не просто решающим, а имеет доминирующее значение. Стремительное развитие отрасли информационно-коммуникационных технологий ведет к увеличению спроса на квалифицированных специалистов в этой сфере. Ведущие мировые производители ведут поиск и подготовку нового поколения исследователей-разработчиков, которые могли бы работать как ученые высшей квалификации и вместе с тем обладали бы желанием видеть практические результаты своих исследований, а также профессиональными навыками, позволяющими добиться этих результатов. Специалисты подобного профиля относятся к научно-технической элите государства, именно они находятся у истока научно-технического прогресса и инновационного развития в сфере информационно-коммуникационных технологий. В связи с этим в настоящее время во всех развитых странах огромное внимание уделяется созданию системы формирования и воспроизводства научно-технической элиты в области высоких технологий, широкое распространение получают имеющие мощную государственную и корпоративную поддержку многоуровневые системы подготовки квалифицированных специалистов в сфере информационно-коммуникационных технологий.

В настоящее время в России всего около 250 из примерно 1000 российских вузов готовят специалистов в области информационно-коммуникационных технологий. Общее число студентов по таким специальностям не превышает 100 тыс. человек (из более чем 3,5 млн студентов, включая заочных). При этом ни один из университетов в России не обеспечивает подготовку специалистов в полном объеме в соответствии с основными международными стандартами.

Основные направления государственной поддержки, реализуемые в рамках Программы, предусматривают следующие направления мер по повышению качества образования:

создание элитарного технологического университета для одаренных студентов, обеспечивающего качество обучения на уровне ведущих университетов мира;

создание на базе технопарков непрерывной «школа-вуз-индустрия» системы подготовки и переподготовки квалифицированных кадров в области информационно-коммуникационных технологий;

модернизация и обновление образовательных стандартов в области подготовки специалистов в сфере информационно-коммуникационных технологий, в соответствии с международными стандартами;

обеспечение государственного заказа на подготовку специалистов в сфере разработки программного обеспечения;

значительное расширение набора студентов по специальностям, связанным с информационно-коммуникационными технологиями, с предоставлением им дополнительных помещений, формирование системы образовательных кредитов, выделение финансовой поддержки студентам, обучающимся по профильным специальностям;

организация на базе высших учебных заведений программ второго высшего образования по специальностям, имеющих высокий спрос в отрасли информационно-коммуникационных технологий;

переподготовка преподавателей в сфере информационно-коммуникационных технологий в соответствии с современными стандартами обучения, включая зарубежные стажировки;

организация сотрудничества учебных заведений с компаниями отрасли, привлечение специалистов к преподаванию, организация для студентов практики и рабочих мест на основе частичной занятости;

внедрение системы государственных гарантий кредитов на обучение за рубежом по наиболее критичным специальностям в области информационно-коммуникационных технологий.

В случае утверждения Программы требуется исключить из состава федеральной целевой программы «Электронная Россия (2002-2010 годы)» мероприятия, имеющие аналогичные задачи.

Для продвижения российской отрасли информационно-коммуникационных технологий необходимо обеспечить реализацию целенаправленной маркетинговой стратегии по созданию и поддержке имиджа России как страны, обладающей квалифицированными кадрами и успешными компаниями, предлагающими конкурентоспособные услуги в этой сфере.

Необходимо также обеспечить поддержку участия российских компаний в важных международных отраслевых мероприятиях (выставках, конференциях, семинарах).

Целесообразным представляется разработка и реализация мер по поддержке российской отрасли информационно-коммуникационных технологий через систему торговых отделов посольств и торговых представительств Российской Федерации за рубежом. Реализация указанных мер может предусматривать информирование о возможностях российских предприятий в этой сфере и сбор данных о потенциальных партнерах в стране расположения торгового представительства.

Следует также организовать государственную поддержку сертификации российских компаний по международным стандартам, которая может включать софинансирование расходов компаний отрасли на получение сертификатов качества, в том числе по стандартам ISO 9001 и CMMi, необходимых для выхода на внешние рынки.

8. Сроки и основные этапы реализации Программы

Программа имеет среднесрочный характер, ее реализация планируется в 2006–2010 годах.

Этапы реализации Программы:

2006 год — создание органов управления реализацией Программы, разработка, подготовка необходимой проектно-сметной и другой документации для организации строительства технопарков в регионах, начало строительства первой очереди объектов создаваемых технопарков, разработка программы продвижения российских предприятий в сфере информационно-коммуникационных технологий на мировой рынок и программы совершенствования системы подготовки кадров в этой сфере, разработка проектной документации создания ведущего технологического университета страны и начало строительства его первой очереди, разработка новых образовательных стандартов для специалистов в сфере информационно-коммуникационных технологий, начало переподготовки и повышения квалификации преподавателей университетов в сфере информационно-коммуникационных технологий.

2007 год — завершение строительства и ввод в действие объектов первой очереди создаваемых технопарков и размещение первых предприятий на их территории, привлечение значительных зарубежных инвестиций в фонд совместного инвестирования и увеличение количества финансируемых перспективных проектов, завершение строительства и ввод в действие первой очереди ведущего технологического университета, конкурсный отбор студентов на его первый курс, апробирование новых образовательных стандартов в основных технологических университетах страны, продолжение программы повышения квалификации преподавателей; начало программы продвижения российских предприятий в сфере информационно-коммуникационных технологий на мировой рынок и привлечение на российский рынок новых заказчиков.

2008 год — начало строительства второй очереди объектов создаваемых технопарков, привлечение ведущих мировых технологических компаний для размещения в технопарках, начало строительства второй очереди ведущего технологического университета страны и проведение следующего набора студентов, распространение новых образовательных стандартов, продолжение программы переподготовки и повышения квалификации преподавателей, продолжение программы продвижения российских предприятий в сфере информационно-коммуникационных технологий на мировой рынок и привлечение на российский рынок новых заказчиков.

2008–2010 годы — завершение строительства и ввод в действие второй очереди объектов создаваемых технопарков, завершение строительства и ввод в действие второй очереди ведущего технологического университета страны, достижение сопоставимого с ведущими мировыми технологическими университетами количества учащихся в нем студентов, обеспечение соответствия общего уровня подготовки специалистов в сфере информационно-коммуникационных технологий российскими вузами ведущим мировым стандартам, выход на стабильно растущие объемы зарубежных заказов.

9. Предложения по объемам, направлениям и источникам финансирования

Необходимый объем финансирования из средств федерального бюджета (млн рублей) в ценах 2005 г.															
Наименование мероприятий	*2006*			*2007*			*2008*			*2009*			*2010*		
	ГКВ	*НИОКР*	*прочие*	*ГКВ*	*НИОКР*	*прочие*	*ГКВ*	*НИОКР*	*прочие*	*ГКВ*	*НИОКР*	*прочие*	*ГКВ*	*НИОКР*	*прочие*
Устранение административных барьеров для развития российских предприятий в сфере ИКТ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Строительство технопарков в сфере ИКТ	2 875	400	250	4 090	264	180	3 100	124	200	2 050	35	140	1 160	18	120
Совершенствование системы подготовки специалистов в сфере ИКТ в соответствии с мировыми стандартами	550	90	370	725	56	350	450	26	330	240	20	320	210	12	340
Продвижение российских предприятий отрасли ИКТ, имеющих высокий экспортный потенциал на мировой рынок			160			150			140			145			152

Структура финансирования программы (млн рублей) в ценах 2005 г.					
	2006	*2007*	*2008*	*2009*	*2010*
Объем финансирования программы:	28 810,2	32 692,6	27 384,9	22 021,5	11 961,2
	4 695,0	5 815,0	4 370,0	2 950,0	2 012,0
средства бюджетов субъектов Российской Федерации	3 615,2	4 477,6	3 364,9	2 271,5	1 549,2
средства внебюджетных источников	20 500,0	22 400,0	19 650,0	16 800,0	8 400,0

10. Оценка ожидаемой эффективности реализации Программы

Занятость в отрасли может составить до 5 процентов работающего населения или 3,5 млн человек. Россия войдет в тройку лидеров на мировом рынке экспорта продукции и услуг в сфере информационно-коммуникационных технологий в 2010 году. Ведущие международные компании откроют в России собственные исследовательские и производственные центры.

Развитие отрасли информационно-коммуникационных технологий будет способствовать повышению производительности труда во всех отраслях экономики, эффективности использования человеческих и материальных ресурсов, что внесет заметный вклад в решение задачи удвоения ВВП и сокращения сырьевой зависимости российской экономики.

Высокий уровень развития информационно-коммуникационных технологий станет важнейшим фактором качественного улучшения систем образования и здравоохранения, реализации проектов адресной социальной поддержки незащищенных слоев населения, обеспечения национальной безопасности на современном уровне.

Другие положительные эффекты от реализации Программы включают увеличение прямых иностранных инвестиций, развитие телекоммуникационной инфраструктуры, повышение общей квалификации специалистов отрасли информационно-коммуникационных технологий.

Рост отрасли приведет к увеличению налогооблагаемой базы. Дополнительные доходы бюджета при этом составят не менее 4 млрд долларов США или 120 млрд рублей в год. Повышение производительности труда в других отраслях в результате внедрения информационно-коммуникационных технологий также увеличит доходы бюджета.

11. Предложения по участию федеральных органов исполнительной власти, ответственных за формирование и реализацию Программы, ее основным государственным заказчикам и разработчикам

Государственных заказчиком — координатором Программы должно стать Министерство информационных технологий и связи Российской Федерации как уполномоченный федеральный орган, ответственный за формирование и реализацию государственной политики в сфере развития и использования информационно-коммуникационных технологий.

Государственными заказчиками Программы должны быть также определены Министерство экономического развития и торговли Российской Федерации, Федеральное агентство по строительству и жилищно-коммунальному комплексу, Федеральное агентство по информационным технологиям, Федеральное агентство по образованию, Федеральное агентство по науке и инновациям, Федеральное агентство по промышленности. Другие государственные заказчики могут быть определены на этапе разработки плана мероприятий программы.

12. Организация управления Программой

Для обеспечения эффективной государственной поддержки развития отечественной отрасли информационно-коммуникационных технологий необходимое управление Программой должно быть возложено на Мининформсвязи России или подведомственные ему федеральные органы исполнительной власти, которые обеспечат координацию работ на межведомственном уровне, планирование и распределение бюджетных средств, а также контроль качества выполнения работ.

При выявлении существенных отклонений от плана достижения намеченных результатов должны быть предусмотрены механизмы оперативного вмешательства в процесс реализации Программы, в том числе, в необходимых случаях, на основе поручений Президента Российской Федерации, Правительства Российской Федерации.

Адрес в Интернете: http://www.minsvyaz.ru/site.shtml?id=3365

УКАЗ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена

В целях обеспечения информационной безопасности Российской Федерации при осуществлении международного информационного обмена посредством информационных систем, сетей и сетей связи, включая международную ассоциацию сетей «Интернет», постановляю:

1. Субъектам международного информационного обмена в Российской Федерации не осуществлять включение информационных систем, сетей связи и автономных персональных компьютеров, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну, и служебная информация ограниченного распространения, а также для которых установлены особые правила доступа к информационным ресурсам, в состав средств международного информационного обмена, в том числе в международную ассоциацию сетей «Интернет» (далее – сеть «Интернет»).

Владельцам открытых и общедоступных государственных информационных ресурсов осуществлять их включение в состав объектов международного информационного обмена только при использовании сертифицированных средств защиты информации, обеспечивающих ее целостность и доступность, в том числе криптографических для подтверждения достоверности информации.

Владельцам и пользователям указанных ресурсов осуществлять размещение технических средств, подключаемых к открытым информационным системам, сетям и сетям связи, используемым при международном информационном обмене, включая сеть «Интернет», вне помещений, предназначенных для ведения закрытых переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну.

2. Службе специальной связи и информации при Федеральной службе охраны Российской Федерации обеспечивать поддержание и развитие сегмента сети «Интернет» для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

3. Администрации Президента Российской Федерации, Аппарату Совета Федерации Федерального Собрания Российской Федерации, Аппарату Государственной Думы Федерального Собрания Российской Федерации, Аппарату Правительства Российской Федерации, аппаратам Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации, Высшего Арбитражного Суда Российской Федерации и Генеральной прокуратуре Российской Федерации осуществлять взаимодействие с сетью «Интернет» и представлять в нее информацию через сегмент сети «Интернет» для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, находящихся в ведении Службы специальной связи и информации при Федеральной службе охраны Российской Федерации.

4. Признать утратившим силу Указ Президента Российской Федерации от 6 октября 1998 г. № 1189 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена».

5. Настоящий Указ вступает в силу со дня его официального опубликования.

Президент Российской Федерации В.Путин

Москва, Кремль
12 мая 2004 года
№ 611

СОДЕРЖАНИЕ

Глава 3
ОТ ЭЛЕКТРОННОЙ КОММЕРЦИИ К ЭЛЕКТРОННОМУ ПРАВИТЕЛЬСТВУ — ЗАРУБЕЖНЫЙ ОПЫТ

Глава 4
ИНФОРМАЦИОННОЕ РАЗВИТИЕ — ПУТЬ КОНКУРЕНТОСПОСОБНОЙ РОССИИ

Глава 5
НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ РОССИИ
В УСЛОВИЯХ ИНФОРМАЦИОННОЙ ГЛОБАЛИЗАЦИИ

CONTENTS

Chapter 3.
FROM E— COMMERCE TO THE E— GOVERNMENT — FOREIGN EXPERIENCE

Chapter 4.
INFORMATION DEVELOPMENT — A WAY TO COMPETITIVE RUSSIA

Анатолий Иванович Смирнов

ИНФОРМАЦИОННАЯ ГЛОБАЛИЗАЦИЯ и РОССИЯ: ВЫЗОВЫ и ВОЗМОЖНОСТИ

Корректура *И.Кохтюлина, А. Сергеева*
Дизайн обложки *И.Кохтюлина*
Компьютерный дизайн и верстка *М. Осипенко*

Подписано в печать 02.09.05. Формат 60x90/16
Печ. л. 24,5. Тираж 3000. Заказ №

Зао «Издательский дом «Парад»
125993, Москва, ул. Правды, 24, офис 811.
Факс (095) 257-43-85, 257-43-69
e-mail: info.parad@mail.ru

Отпечатано .....