МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования**
«Нижегородский государственный университет им. Н.И. Лобачевского»

Факультет международных отношений
Кафедра прикладной политологии

**А.Е. Белянцев**

*Учебно-методический комплекс (УМК) по дисциплине*

# КОММУНИКАЦИИ И КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В СОВРЕМЕННЫХ ПОЛИТИЧЕСКИХ ПРОЦЕССАХ

Рекомендовано методической комиссией факультета международных отношений для студентов ННГУ, обучающихся по направлению подготовки *031900.62 «Международные отношения»*

Нижний Новгород
2013 г.

**СОДЕРЖАНИЕ**

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## 1. Цели освоения дисциплины

**Целью данной дисциплины** является комплексная оценка влияния новейших информационных технологий на современные политические процессы.

Процесс реализация поставленной цели предполагает **решение ряда задач:**

- усвоение студентами основ теории информационных систем, а также специфики ее применения в сфере политики;
- усвоение студентами базовых моделей политической коммуникации, а также изучение некоторых значимых особенностей практики политических коммуникаций в условиях информационной революции;
- изучение теоретических концепций постиндустриального (информационного) общества;
- изучение влияния глобальной информационной революции на институт государства, современные международные конфликты, терроризм и преступность;
- формирование представления об информационной безопасности на международном и национальном уровнях;
- проведение сравнительного анализа информационной политики различных государств мира;
- изучение применения новых компьютерных технологий в политической практике, а также в процессе информационно–аналитической деятельности.

## 2. Место дисциплины в структуре ООП

Данная учебная дисциплина входит в вариативную часть математического и естественнонаучного цикла ООП (основной образовательной программы) бакалавриата направления «Международные отношения».

Для изучения дисциплины необходимы компетенции, сформированные в результате освоения таких дисциплин ООП бакалавриата, как «Информатика» и «Концепции современного естествознания».

В рамках освоения дисциплин ООП курс «Коммуникации и компьютерные технологии в современных политических процессах» показывает место и роль информации в мировой политике, подготавливает к более осознанному освоению профессиональных компетенций, связанных с современными коммуникационными и информационно-аналитическими технологиями. Кроме того, данная учебная дисциплина предваряет большинство курсов профессионального цикла, предусматривающих учет информационного фактора при изучении ряда своих разделов.

## 3. Требования к результатам освоения дисциплины (модуля)

Изучение дисциплины нацелено на формирование следующих общекультурных и профессионально-дисциплинарных компетенций:

умение использовать основные законы естественно-научных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования (ОК-11);

способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (ОК-12);

владение основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-13);

способность работать с информацией в глобальных компьютерных сетях (ОК-14).

умение понимать и анализировать мировоззренческие, социально и личностно значимые философские проблемы (ОК-17);

понимание структуры глобальных процессов научно-технологических инноваций и перспектив изменения в них места и роли России (ПДК-4).

**В результате освоения дисциплины студенты должны:**

- **Знать и уметь** анализировать результаты и последствия информационной революции для мировой политической системы.
- **Иметь представление** об основных теоретических моделях и концепциях информационного общества, политической коммуникации, информационных войн, информационной безопасности, а так же международно-правовом регулировании глобальной инфосферы.
- **Обладать навыками** применения новых компьютерных технологий в политической практике, а так же в процессе информационно–аналитической деятельности.

## 4. Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 1 зачетная единица (36 ч.).

| № п/п | Раздел дисциплины | Семестр | Недели семестра | Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах) | | | Формы текущего контроля успеваемости *(по неделям семестра)* |
|---|---|---|---|---|---|---|---|
| | | | | Лекции | Семинары | СР | |
| 1. | Введение. Информация, управление, коммуникация и политическая коммуникация. Мировая политическая система в информационную эпоху: основные тенденции. | 4 | 1 | 2 | - | 2 | |
| 2. | Информационное общество: теоретическая модель или реальность? Анализ результатов и последствий информационной революции. | 4 | 3 | 2 | - | 2 | |
| 3. | Интернет как глобальная информационная среда. Интернет в современной мировой политике. | 4 | 5 | 2 | - | 2 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4. | Опыт и проблемы становления глобального информационного общества. Информационное «измерение» международной безопасности. Современный мировой информационный порядок: правовые аспекты. «Информационное общество» как политическая задача и международный проект. ИТ-проекты по развитию глобального информационного общества. | 4 | 7 | 2 | - | 2 | Письменная работа № 1 |
| 5. | Информационные войны: теоретические концепции и боевые операции. Компьютерная преступность и компьютерный терроризм. | 4 | 9 | 2 | - | 2 | |
| 6. | Информационная политика: мировой опыт. Особенности современной информационной политики Российской Федерации. | 4 | 11 | 2 | - | 2 | |
| 7. | Информационная безопасность современного государства. Основные направления обеспечения информационной безопасности Российской Федерации. | 4 | 13 | 2 | - | 2 | |
| 8. | Политическая коммуникация в информационном обществе. Новые информационные технологии в политической практике. Компьютерные технологии в информационно–аналитической деятельности. | 4 | 15 | 2 | - | 2 | Письменная работа № 2 |
| **ИТОГО за семестр:** | | | | **16 ч.** | **-** | **16 ч.** | |

## Технологическая карта дисциплины

| №п/п | Раздел дисциплины | Информативные лекции | Интерактивные лекции-консультации |
|---|---|---|---|
| 1. | Информация, управление, коммуникация и политическая коммуникация. Мировая политическая система в информационную эпоху: основные тенденции. | 2 ч. | - |
| 2. | Информационное общество: теоретическая модель или реальность? Анализ результатов и последствий информационной революции. | - | 2 ч. |
| 3. | Интернет как глобальная информационная среда. Интернет в современной мировой политике. | 2 ч. | - |
| 4. | Опыт и проблемы становления глобального информационного общества. Информационное «измерение» международной безопасности. Современный мировой информационный порядок: правовые аспекты. «Информационное общество» как политическая задача и международный проект. ИТ-проекты по развитию глобального информационного общества. | - | 2 ч. |
| 5. | Информационные войны: теоретические концепции и боевые операции. Компьютерная преступность и компьютерный терроризм. | 2 ч. | - |
| 6. | Информационная политика: мировой опыт. Особенности современной информационной политики Российской Федерации. | - | 2 ч. |
| 7. | Информационная безопасность современного государства. Основные направления обеспечения информационной безопасности Российской Федерации. | 2 ч. | - |
| 8. | Политическая коммуникация в информационном обществе. Новые информационные технологии в политической практике. Компьютерные технологии в информационно–аналитической деятельности. | - | 2 ч. |
| | **ИТОГО за семестр:** | **8 ч.** | **8 ч.** |

## 5. Образовательные технологии

Используемые образовательные технологии: информативные и проблемные лекции, интерактивные лекции-консультации.

Особое место в освоении дисциплины отводится интерактивным лекциям-консультациям, на которых студенты работают с аналитическими материалами, текстами, статьями и т. п., овладевая знаниями и понятийным аппаратом по проблематике курса. В ходе реализации программы курса используется технология развития критического

мышления.

Внеаудиторная самостоятельная работа студента ориентирована на подготовку к лекциям в виде поиска информации по предложенным вопросам для обсуждения, а так же на выполнение итоговых индивидуальных письменных работ.

Удельный вес занятий, проводимых в интерактивных формах, составляет не менее 50% аудиторных занятий.

## 6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Контроль самостоятельной работы (КСР) студентов осуществляется на лекциях-консультациях. КСР включает устные доклады в ходе лекций-консультаций, в рамках тем, указанных в разделе 4 данной программы, а так же две творческие письменные работы – аналитические обзоры источников и/или литературы в рамках тематики курса (**контроль:** 7-ая и 15-ая недели семестра).

Уровень усвоения дисциплины на положительную оценку («зачтено») предполагает посещение не менее половины занятий и успешное выполнение не менее половины предусмотренных форм КСР. В случае невыполнения названных требований и отказа от отработки текущей задолженности в установленное время студент не допускается к сдаче зачета.

### Вопросы для итогового контроля по дисциплине

1. Информация. Роль и функции информации. Система. Понятие информационной системы. Классификация информационных систем. Структура информационной системы как совокупность обеспечивающих подсистем (информационное, техническое, программно-математическое и организационно-правовое обеспечение). Процессы в информационной системе. Обратная связь. Управление и принятие решений. Влияние новых информационных технологий на процессы управления и принятия решений.
2. Понятие коммуникации и политической коммуникации. Модели политической коммуникации. Процесс политической коммуникации. Информационно-коммуникативные системы (ИКС). Система современных международных отношений в качестве ИКС.
3. Становление глобального информационного общества. Глобализация как процесс формирования единого общемирового финансово-информационного пространства. Информационная революция (качественно новый этап развития и внедрения информационных технологий) и современный мировой политический процесс (МПП). Три составляющие МПП (субъекты МПП – мировое сообщество; содержательная сторона МПП, т.е. международные отношения; безопасность) и последствия информационной революции.
4. Международно-значимые результаты трансграничного информационного обмена. Децентрализация, прозрачность границ, плюрализм; появление новых негосударственных акторов (структур и субъектов глобального информационного пространства), действующих в международном масштабе, сетевая организация сообществ.

5. Новая экономика информационной эпохи: снижение возможностей государственного управления и контроля в экономической сфере.
6. Государственный суверенитет в условиях глобализации и информационной революции: адаптация государства к новым условиям.
7. Электронно-цифровой разрыв и его последствия для мирового сообщества.
8. Влияние информационных технологий на процесс принятия политических решений. Виртуальное международное сотрудничество – новый ресурс человечества.
9. Возрастание роли информационной составляющей структуры международной безопасности. Изменение форм международных конфликтов.
10. Футурологические концепции постиндустриального (информационного) общества. Основные черты информационного общества (по работам Д. Белла, А. Тоффлера, М. Кастельса, Ф. Фукуямы и др.).
11. Информационная революция и «новая экономика». Государство и власть, социальная структура, международные отношения в эпоху постиндустриализма. Римский клуб об информационном обществе. Глобальная «инфосфера» как фактор трансформирующий современную цивилизацию.
12. «Информационная эпоха»: сбылись ли предсказания футурологов?
13. Возникновение и развитие сети Интернет.
14. Формирование глобального трансграничного виртуального пространства. Интернет в экономике, социальной, политической и культурной жизни. Интернет и качественная революция в образовании.
15. Влияние сети Интернет на формирование «глобального гражданского общества». Сетевые интернет-сообщества – новые действующие лица современной мировой политики.
16. Глобальная компьютерная сеть Интернет как важнейшая составляющая инфраструктуры постиндустриального (информационного) общества.
17. Системный подход к проблемам безопасности. Изменение системных свойств современного мира, связанное с усложнением систем (примеры). Появление новых (системных) свойств у сложных систем (у целого появляются свойства, которыми не обладают части), с которыми связаны как новые ресурсы развития системы, так и новые источники угроз безопасности. Воздействие на информационную систему (сильное и слабое). Комплексный подход к обеспечению безопасности сложных систем.
18. Тенденция к усложнению мировой политической системы в процессе глобализации. Глобализация и международная безопасность. Возрастание роли невоенных составляющих безопасности. Информационная безопасность – важнейшая составляющая структуры международной безопасности.
19. «Реалистический» и «либеральный» подходы к проблеме информационной безопасности в современных международных отношениях. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Обзор и характеристика новых видов угроз международной безопасности: распространение «метатехнологий»; электронно-цифровой разрыв; информатизационная милитаризация; компьютерная преступность и компьютерный терроризм.
20. Необходимость международно-правового регулирования процессов гражданской и военной информатизации. Резолюция ООН 54/49 и ее значение для мирового сообщества. Деятельность ООН в области регулирования информационной сферы.
21. Окинавская Хартия Глобального Информационного Общества: всесторонний анализ современной инфосферы, определение возможных путей международного сотрудничества в киберпространстве и попытка правового регулирования процесса глобальной информатизации. Деятельность G 7/8 в области регулирования информационной сферы.
22. ВВУИО как механизм регулирования и организации структур глобального информационного общества.

23. Другие международные (многосторонние и двусторонние) правовые акты в информационной сфере. Формирование международного информационного законодательства.
24. Конфликты и войны в условиях глобальной информатизации. Война в заливе (1991) как первый конфликт информационной эпохи. Революция в военном деле. Киберпространство - новое поле боя. Изменение традиционных военных теорий, стратегии и тактики ведения боевых действий. Распределенная военная операция. Международный конфликт как глобальная информационная война.
25. Определение информационной войны и информационного оружия согласно документам ООН. Классификация информационного оружия. Информационное оружие прямого и общего назначения. Особенности информационного оружия.
26. Теория информационной войны (по работам М. Либики, Д. Альбертса, У. Швартау и др.): военные функции информации; определение информационной войны; составные части (формы) информационной войны; виды информационных атак; оборонная сторона информационной войны; цели информационной войны. Особенности информационных атак. Асимметричный характер противоборства. Нетрадиционные акторы (действующие лица) в информационном противоборстве. Задачи нападающей и обороняющейся сторон. Классификация наиболее уязвимых (по отношению к информационному нападению) технологий, систем и структур.
27. Новейшие концепции сетевой войны и кибервойны. Сете-центрическая война.
28. Проект создания объединенного информационного корпуса в вооруженных силах США. Усложнение стратегической формулы: от C2 (command and control) через C3I (command, control, communications and intelligence) к C4I2 (command, control, communications, computers, intelligence and interoperability).
29. Информационно-психологическая война в глобальных СМИ, сопровождающая современные международные конфликты. Вмешательство СМИ в ход конфликта: эффект CNN, эффект режима реального времени, информационная прозрачность современных конфликтов, формирование общественного мнения в глобальном масштабе посредством СМИ. Управление информационным обеспечением военной кампании. Разработка общей концепции освещения военного конфликта с применением коммуникативных технологий.
30. Стратегическая концепция НАТО и военная доктрина США об информационных войнах.
31. Региональные конфликты в Персидском заливе (1991), в Югославии (1998-1999), в Ираке (2003), в Южной Осетии (2008) и др. как информационные войны. Контртеррористическая операция в Афганистане (2001-2002) как пример сетевой войны. Уроки для России.
32. Психологические операции. Информационно-психологическая война СССР - Запад: результаты и последствия.
33. Технологии «high-hume» (технологии организации и управления): примеры и потенциальная опасность.
34. Компьютерный терроризм и компьютерная преступность: примеры, причины возникновения, основные тенденции.
35. Информационная политика. Концептуальные принципы формирования информационной политики государства.
36. Национальные модели информационного общества и опыт их реализации. Сравнительный анализ информационной политики различных государств мира: опыт США, опыт стран Европейского сообщества, опыт Японии, опыт КНР, опыт стран Восточной Азии, опыт исламских государств и др. Уроки для России.
37. Социальные предпосылки и особенности становления информационного общества в России. Развитие в России информационной и коммуникационной инфраструктуры. Государственная информационная политика России. Проблемы и перспективы интеграции России в мировое информационное общество.

38. Информационная сфера (информационное пространство) - системообразующий фактор жизнедеятельности современного государства. Появление принципиально новых угроз безопасности государства.
39. Основные определения и терминология. Информационная безопасность государства - комплекс мер по защите суверенитета национального информационного пространства. Соотношение информационной безопасности и национальных интересов государства. Информационная среда государства. Угрозы национальной безопасности в информационной сфере: определение и классификация.
40. Грани информационной безопасности. Необходимость комплексного (системного) подхода к обеспечению информационной безопасности государства. Основные категории интересов субъектов информационного пространства: доступность информации (возможность за приемлемое время получить требуемую информационную услугу); целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения); конфиденциальность информации (защита от несанкционированного ознакомления).
41. Уровни информационной безопасности: законодательный (законы, нормативные акты, стандарты и т.п.); административный (действия общего характера, предпринимаемые руководством); процедурный (конкретные меры безопасности, имеющие дело с людьми); программно-технический (конкретные технические меры).
42. Место и роль информационной безопасности в обновленной концепции национальной безопасности РФ (2000). Основы национальной безопасности РФ в информационной сфере.
43. Доктрина информационной безопасности РФ: национальные интересы РФ в информационной сфере; объекты обеспечения информационной безопасности; внешние и внутренние угрозы национальной безопасности в информационной сфере; международное сотрудничество РФ в области обеспечения информационной безопасности.
44. Обзор законодательства РФ в области защиты информации.
45. Региональная информационная безопасность.
46. Электронная (цифровая) дипломатия. Электронное правительство. Электронная демократия.
47. Понятие Интернет-СМИ, правовое регулирование и разновидности интернет-СМИ. Особенности ведения агитации в интернет-СМИ. История создания и развития интернет-СМИ в России. Блоги и «блогосфера».
48. Влияние новых информационных технологий на выборы. PR и реклама в информационном обществе.
49. Информационное управление: потенциальные возможности и опасности.
50. «Глобальное управление» в контексте информационной революции.
51. Технологии управления взаимоотношениями с населением (CRM). Геоинформационные технологии. WWW-технологии. Технологии аналитической обработки информации. Современные технологии совместной работы. Технологии построения и эксплуатации хранилищ информации. Технологии ситуационного управления. Social software (управление сообществами через интернет).
52. Цели, задачи, объект, предмет, субъекты информационно-аналитической деятельности. Сущность и содержание информационно-аналитической деятельности.
53. Методы анализа, связанные с использованием новых информационных технологий. Сбор информации с использованием сети Интернет. Роль информации, собираемой из открытых источников.

## Критерии оценок

| | |
|---|---|
| **Зачтено** | подготовка, удовлетворяющая минимальным требованиям или выше |
| **Не зачтено** | необходима дополнительная подготовка для успешного прохождения испытания |

## 7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) основная литература:


1. Балуев Д.Г. Завоевание будущего: внешняя политика России на рубеже веков: Монография. - Н.Новгород: ИСИ ННГУ,1999. - 122 с.
2. Балуев Д.Г. Информационная революция и современные международные отношения: Уч. пособие. - Н.Новгород: ННГУ, 2001. - 107 с.
3. Балуев Д.Г. Новые информационные технологии и современные международные отношения. - Н.Новгород: ННГУ, 1998. - 47 с.
4. В.Л. Иноземцев. Современное постиндустриальное общество. - М.: Логос, 2000.
5. Колобов О.А., Ясенев В.Н. Информационная безопасность и антитеррористическая деятельность современного государства: Проблемы правового регулирования и варианты их решения: Уч. пособие. - Н.Новгород: ННГУ, 2001. - 374 с.
6. Лисичкин В.А., Шелепин А.А. Третья мировая (информационно-психологическая) война. - М.: Институт социально-политических исследований АСН, 2000. - 304 с.
7. Модестов С.А. Информационное противоборство как фактор геополитической конкуренции. (Серия «Научные доклады», вып. 74.) - М.: МОНФ; Издательский центр научных и учебных программ, 1999. - 64с.
8. Новая постиндустриальная волна на Западе. Антология/ Под ред. В.Л. Иноземцева. - М.: Academia, 1999.
9. Почепцов Г.Г. Информационно-психологическая война. - М.: СИНТЕГ, 2000. - 180 с.
10. Расторгуев С.П. Философия информационной войны. - М.: Вузовская книга, 2001. - 468 с.
11. Слипченко В.И. Война будущего. (Серия «Научные доклады», вып. 88.) - М.: МОНФ; Издательский центр научных и учебных программ, 1999. - 292с.
12. Современная западная философия: Словарь/ Сост.: Малахов В.С., Филатов В.П. - М.: Политиздат, 1991. - 414 с.


б) дополнительная литература:


13. Абдеев Р.Ф. Философия информационной цивилизации. - М., 1994.
14. Анохин М.Г., Комаровский В.С. Политика: возможность современных технологий. - М.,1998.
15. Анохин М.Г., Павлютенкова М.Ю. Информационно-коммуникативные технологии в политике. // Вестник Российского университета дружбы народов. – Сер.: Политология. – 1999. – № 1.
16. Анохин М.Г.Компьютерные технологии в политике и политологии. // Общая и прикладная политология: Учебное пособие / Общ. ред.: Жуков В.И., Краснов Б.И. – М., 1997. С.760-771.
17. Багиров А. Новые информационные технологии в международных отношениях. // Международная жизнь, 2001, №8.
18. Белл Д. Грядущее постиндустриальное общество. - М.: Academia, 1999.

19. Братимов О.В., Горский Ю.М., Делягин М.Г., Коваленко А.А. Практика глобализации: игры и правила новой эпохи. - М.: ИНФРА-М, 2000. - 344 с.
20. Василенко В.И., Василенко Л.А. Интернет в системе государственной службы. - М., 1998.
21. Васильев Г.Г. Становление информационной цивилизации и тенденции обновления регулятивной системы общества. // Роль государства в формировании современного общества. - М., 1998.
22. Васкевич Д. Стратегии клиент/сервер. Руководство по выживанию для специалистов по реорганизации бизнеса. - К.: Диалектика, 1996. - 384 с.
23. Введение в философию: Учебник для вузов. В 2 ч./ Под общ. Ред. И.Т. Фролова. - М.: Политиздат, 1989.
24. Воронина Т.П. Информационное общество: сущность, черты, проблемы. - М., 1995.
25. Гаджиев К.С. Введение в политическую науку: Учебник для вузов. - М.: Логос, 1999. - 544 с.
26. Григорьев М.С. Политические коммуникации в "век информации". // Политическое управление: Сборник научных трудов кафедры политологии и политического управления. - М., 1998.
27. Гудков В.В. Государство и информационное общество. // Труды Московской государственной юридической академии. - 1999. - № 4.
28. Дайсон Э. Жизнь в эпоху Интернета. Release 2.0. - М.: Бизнес и Компьютер, 1998. - 400 с.
29. Даниелов А.Р. Россия в мировой системе высоких технологий: формирование информационного общества. // США: Экономика, политика, идеология. - 1996. - № 9.
30. Дмитриев А.В., Латынов В.В., Хлопьев А.Т. Неформальная политическая коммуникация.—М., 1996.
31. Доброхотов Р.А. Политика в информационном обществе. // Полис, 2004, №3.
32. Егоров В.С. Человек информационный. // Человек, наука, управление. - М., 2000.
33. Егоров Э.Н. Информационное общество. М., 1993.
34. Запад: новые измерения национальной и международной безопасности: Монография. - Н.Новгород: ННГУ, 1997. - 348 с.
35. Иларионова Т.С. Информационные процессы в современной России. - М., 1999.
36. Иноземцев В.Л. Современное индустриальное общество: природа, противоречия, перспективы. - М., 2000.
37. Информационная технология и информационная политика. Научно-информационное исследование. / Редколлегия: В.А.Виноградов (гл.ред.) и др. Научный руководитель Ракитов А.И. - М.: ИНИОН РАН (Информация, наука, общество), 1994.
38. Информационное обеспечение государственного управления. / Авт.: Никитов В.А., Орлов Е.И., Старовойтов А.В., Савин Г.И.; Под ред. Ю.В.Гуляева. - М., 2000.
39. Канке А.А., Лобачев В.В. Информационные технологии как основа системной интеграции. // Наука управления на пороге XXI века. Материалы международной научной конференции. /ГАУ. - М., 1997.
40. Кастельс М. Информационная эпоха: Экономика, общество и культура. М., 2000.
41. Кашлев Ю. Международные отношения в зеркале информационной революции. // Международная жизнь, 2003, №1.
42. Кедровский О.В. Информационная среда обитания. // Информационные ресурсы России. - 1995. - № 3.
43. Кеннеди П. Вступая в двадцать первый век. - М.: Весь Мир, 1997. - 480 с.
44. Клепцов М.Я. Информационные системы органов государственного управления. - М., 1996.
45. Колин К.К. Наука для будущего: социальная информатика. // Информационные ресурсы России. - 1995. - № 3.
46. Компьютеризация общества и человеческий фактор. Реферативный сборник/ Отв. Ред. А.И. Ракитов. - М.: ИНИОН АН СССР, 1988. - 228 с.

47. Кристиансон М. Подход к анализу информационной политики, основанный на изменениях в глобальных экономических силах // Международный форум по информации и документации. - 1996. - т.21. - №1.
48. Лагутина М.Л. Объективные условия формирования глобальной системы. // Россия в глобальном мире. Ч.1. СПб., 2004.
49. Лагутина М.Л. Роль глобализации в формировании новой системы международных отношений. // Россия в глобальном мире. СПб., 2006.
50. Леонов Н.С. Информационно-аналитическая работа в загранучреждениях. М., 1996.
51. Лукницкий С.П. Средства массовой информации в системе социального управления современной России: автореф.д.с.н..—М., 1998.
52. Манойло А.В. Государственная информационная политика в особых условиях. Монография. М., 2003.
53. Международная конференция «Глобальные проблемы как источник чрезвычайных ситуаций» 22-23 апреля 1998 г. Доклады и выступления/ Под ред. Воробьева Ю.Л. - М.: УРСС, 1998. - 320 с.
54. Мелюхин И.С. Информационное общество: истоки, проблемы, тенденции развития. - М., 1999.
55. Мешкова Т.А. Социально-политические аспекты глобальной информатизации // Полис. - 2002. - N 6.
56. Моисеев Н. Информационное общество как этап новейшей истории. // Свободная мысль, 1996, №1.
57. Мур Н. Права и обязанности в информационном обществе. // Научные и технические библиотеки. - 1999. - № 1.
58. Мухин А.А. Информационная война в России.—М., 2000.
59. «Мягкие» и «жесткие» вызовы безопасности в Приволжском федеральном округе: Аналитический доклад/ Под ред. проф. А.С. Макарычева. - Н.Новгород: НГЛУ, 2001. - 164 с.
60. Нисневич Ю.А. Информационная политика России: проблемы и перспективы. - М., 1999.
61. Нисневич Ю.А. Информация и власть. - М., 2000.
62. Панарин И.Н. Информационная война и Россия.—М.. 2000.
63. Пасхин Е.Н. Информатизация образования в стратегии устойчивого развития: философско-методологический анализ. - М., 1999.
64. Перфильев Ю.Ю. Российское Интернет-пространство: развитие и структура. М., 2003.
65. Политология и международные отношения в современной высшей школе: проблемы организации учебного процесса и осуществления фундаментальных научных исследований: Материалы международной научно-практической конференции. - Н.Новгород: ИСИ ННГУ, 1999. - 264 с.
66. Политология. Учебник/ Отв. редактор В.М. Утенков. - М.: Редакционно-издательский центр МГОПУ, 2000. - 438 с.
67. Попов В.Д. Информациология и информационная политика. - М., 2001.
68. Поппель Г., Голдстайн Г. Информационная технология - миллионные прибыли. - М.: Экономика, 1990. - 238 с.
69. Постиндустриальный мир: Центр, Периферия, Россия. Общие проблемы постиндустриальной эпохи. (Серия «Научные доклады», вып. 91.) - М.: МОНФ; ИМЭМО РАН, 1999. - 304с.
70. Постиндустриальный мир: Центр, Периферия, Россия. Особый случай России. (Серия «Научные доклады», вып. 93.) - М.: МОНФ; ИМЭМО РАН, 1999. - 224с.
71. Почепцов Г.Г. Коммуникативные технологии XX века. - М., 1999.
72. Прайс Монро. Телевидение, телекоммуникации и переходный период: право, общество и национальная идентичность.- М., 2000.
73. Проблема трансграничности информации. Интеграция пространства и сетевая несвобода. // МЭМО, 2000, №11.

74. Пугачев В.П. Средства массовой коммуникации в современном политическом процессе // Вестник МГУ. - Серия 12: Политические науки. - 1995. - № 5.
75. Ракитов А.И. Информация, наука, технология в глобальных исторических изменениях. - М.,1998.
76. Ракитов А.И. Философия компьютерной революции. - М., 1991.
77. Римский клуб/ Сост. Д.А. Гвишиани, А.И. Колчин, Е.В. Нетесова, А.А. Сейтов. - М.: УРСС, 1997. - 384 с.
78. Россия - США - НАТО: динамика современных взаимоотношений и возможности преодоления кризиса доверия/ Под общ. ред. О.А. Колобова. - Москва - Н.Новгород: АВН РФ; РАЕАС; ИСИ ННГУ, 2000. - 243 с.
79. Россия и НАТО после Балканского кризиса: Материалы международной научной конференции. - Н.Новгород: ННГУ, 2000. - 112 с.
80. Россия: стратегия достоинства. Имидж и реальность страны, информационные технологии и кризисные ситуации /Под ред.: С.Е.Кургиняна и А.П.Ситникова.—М., 2001.
81. Сидоров В.А. Политическая культура средств массовой информации. - М., 1994.
82. Симоненко В.Б. Новые информационные технологии и политика. // Общая и прикладная политология: Учебное пособие / Общ. ред.: Жуков В.И., Краснов Б.И. – М., 1997. С.752-759.
83. Смолян Г.Л., Черешкин Д.С., Вершинская О.Н., Костюк В.Н., Савостицкий Ю.А. Путь России к информационному обществу (предпосылки, проблемы, индикаторы, особенности). - М., 1997. Совершенствование государственного управления на основе его реорганизации и информатизации. Мировой опыт. - М., 2002.
84. Стоуньер Т. Информационное богатство: профиль постиндустриальной экономики // Новая технократическая волна на Западе. - М., 1986.
85. США 80-х: взгляд изнутри. «Американская модель»: с будущим в конфликте/ Под общ. ред. Г.Х. Шахназарова. - М.: Прогресс, 1984. - 256 с.
86. Технологии в политике и политическом управлении. / Под ред. Анохина М.Г., Комаровского В.С., Матвеенко Ю.И. - М., 2000.
87. Тоффлер А. Смещение власти: знание, богатство и принуждение на пороге XXI века. - М., 1991.
88. Тоффлер А. Третья волна. - М.: АСТ, 1999. - 748 с.
89. Уэбстер Ф. Теории информационного общества. М., 2004.
90. Философский энциклопедический словарь/ Гл. редакция Л.Ф. Ильичев, П.Н. Федоров, С.А. Ковалев, В.Г. Попов. - М.: Сов. Энциклопедия, 1983. - 840 с.
91. Хакен Г. Информация и самоорганизация. - М.: Мир, 1991.
92. Хохлышева О.О. Разоружение, безопасность, миротворчество: Глобальный масштаб. - Москва - Н.Новгород: АВН РФ; АНМ «Элита» при ООН; ИСИ ННГУ, 2000. - 308 с.
93. Шретмен К.А. Управление информацией в 90-е годы: концептуальные основы. // Международный форум по информации и документации. - 1993. - № 2. - Т. 18.
94. Юзвишин И.И. Основы информациологии. - М., 2000.
95. Addington, Larry H. The patterns of war since the eighteenth century. - Bloomington and Indianapolis: Indiana University Press, 1994. - 362 p.
96. Alberts, David S. Defencive information warfare. - Washington DC: NDU Press, 1996. - 82 p.
97. De Landa, Manuel. War in the age of intelligent machines. - New York: Swereve Editions, 1991. - 272 p.
98. Libicki, Martin C. Defending cyberspace and other metaphors. - Washington DC: NDU Press, 1997. - 110 p.
99. Libicki, Martin C. What is information warfare? - Washington DC: NDU Press, 1995. - 104 p.
100. Shukman, David. Tomorrow’s war: the threat of high-technology weapons. - New York/San Diego/London: Hardcourt Brace&Company, 1996. - 272 p.
101. Van Creveld, Martin. Technology and war: from 2000 B.C. to the present. - New York: The Free Press. 1991. - 342 p.

102. War in the information age: new challenges for US security policy/ edited by Robert L. Pfalzgraff, Jr, Richard Shultz, Jr. - Washington/London: Brassey's, 1997. - 376 p.

**Кроме предлагаемой литературы студентам рекомендуется широко использовать периодические издания и электронные публикации в сети Internet.**

## 8. Материально-техническое обеспечение дисциплины (модуля)

Ноутбук, проектор, интерактивная доска, экран для презентаций на аудиторных занятиях.

Компьютерный класс с доступом к сети Интернет для практических занятий и внеаудиторной самостоятельной работы.

# КРАТКИЕ КОНСПЕКТЫ ИНФОРМАТИВНЫХ ЛЕКЦИЙ

*Лекция №1*

**Информация, управление, коммуникация и политическая коммуникация.**

Информация. Роль и функции информации. Система. Понятие информационной системы. Классификация информационных систем. Структура информационной системы как совокупность обеспечивающих подсистем (информационное, техническое, программно-математическое и организационно-правовое обеспечение). Процессы в информационной системе. Обратная связь. Управление и принятие решений. Влияние новых информационных технологий на процессы управления и принятия решений.

Понятие коммуникации и политической коммуникации. Модели политической коммуникации. Процесс политической коммуникации. Информационно-коммуникативные системы (ИКС). Система современных международных отношений в качестве ИКС.

Становление глобального информационного общества.

**Мировая политическая система в информационную эпоху: основные тенденции.**

Глобализация как процесс формирования единого общемирового финансово-информационного пространства. Информационная революция (качественно новый этап развития и внедрения информационных технологий) и современный мировой политический процесс (МПП). Три составляющие МПП (субъекты МПП – мировое сообщество; содержательная сторона МПП, т.е. международные отношения; безопасность) и последствия информационной революции.

Международно-значимые результаты трансграничного информационного обмена.

Децентрализация, прозрачность границ, плюрализм; появление новых негосударственных акторов (структур и субъектов глобального информационного пространства), действующих в международном масштабе, сетевая организация сообществ.

Новая экономика информационной эпохи: снижение возможностей государственного управления и контроля в экономической сфере.

Государственный суверенитет в условиях глобализации и информационной революции: адаптация государства к новым условиям.

Электронно-цифровой разрыв и его последствия для мирового сообщества.

Влияние информационных технологий на процесс принятия политических решений. Виртуальное международное сотрудничество – новый ресурс человечества.

Возрастание роли информационной составляющей структуры международной безопасности. Изменение форм международных конфликтов.

*Лекция №2*

**Интернет как глобальная информационная среда. Интернет в современной мировой политике.**

Возникновение и развитие сети Интернет.

Формирование глобального трансграничного виртуального пространства. Интернет в экономике, социальной, политической и культурной жизни. Интернет и качественная революция в образовании.

Влияние сети Интернет на формирование «глобального гражданского общества». Сетевые интернет-сообщества – новые действующие лица современной мировой политики.

Глобальная компьютерная сеть Интернет как важнейшая составляющая инфраструктуры постиндустриального (информационного) общества.

*Лекция №3*

**Информационные войны: теоретические концепции.**

Конфликты и войны в условиях глобальной информатизации.

Война в заливе (1991) как первый конфликт информационной эпохи. Революция в военном деле. Киберпространство - новое поле боя. Изменение традиционных военных теорий, стратегии и тактики ведения боевых действий. Распределенная военная операция. Международный конфликт как глобальная информационная война.

Определение информационной войны и информационного оружия согласно документам ООН. Классификация информационного оружия. Информационное оружие прямого и общего назначения. Особенности информационного оружия.

Теория информационной войны (по работам М. Либики, Д. Альбертса, У. Швартау и др.): военные функции информации; определение информационной войны; составные части (формы) информационной войны; виды информационных атак; оборонная сторона информационной войны; цели информационной войны. Особенности информационных атак. Асимметричный характер противоборства. Нетрадиционные акторы (действующие лица) в информационном противоборстве. Задачи нападающей и обороняющейся сторон. Классификация наиболее уязвимых (по отношению к информационному нападению) технологий, систем и структур.

Новейшие концепции сетевой войны и кибервойны. Сете-центрическая война.

Проект создания объединенного информационного корпуса в вооруженных силах США. Усложнение стратегической формулы: от C2 (command and control) через C3I (command, control, communications and intelligence) к C4I2 (command, control, communications, computers, intelligence and interoperability).

Информационно-психологическая война в глобальных СМИ, сопровождающая современные международные конфликты. Вмешательство СМИ в ход конфликта: эффект CNN, эффект режима реального времени, информационная прозрачность современных конфликтов, формирование общественного мнения в глобальном масштабе посредством СМИ. Управление информационным обеспечением военной кампании. Разработка общей концепции освещения военного конфликта с применением коммуникативных технологий.

**Информационные войны: боевые операции.**

Стратегическая концепция НАТО и военная доктрина США об информационных войнах.

Региональные конфликты в Персидском заливе (1991), в Югославии (1998-1999), в Ираке (2003), в Южной Осетии (2008) и др. как информационные войны. Контртеррористическая операция в Афганистане (2001-2002) как пример сетевой войны. Уроки для России.

Психологические операции. Информационно-психологическая война СССР - Запад: результаты и последствия.

Технологии «high-hume» (технологии организации и управления): примеры и потенциальная опасность.

**Компьютерная преступность и компьютерный терроризм.**

Компьютерный терроризм и компьютерная преступность: примеры, причины возникновения, основные тенденции.

*Лекция №4*

**Информационная безопасность современного государства.**

Информационная сфера (информационное пространство) - системообразующий фактор жизнедеятельности современного государства. Появление принципиально новых угроз безопасности государства.

Основные определения и терминология. Информационная безопасность государства - комплекс мер по защите суверенитета национального информационного пространства. Соотношение информационной безопасности и национальных интересов государства.

Информационная среда государства. Угрозы национальной безопасности в информационной сфере: определение и классификация.

Грани информационной безопасности. Необходимость комплексного (системного) подхода к обеспечению информационной безопасности государства. Основные категории интересов субъектов информационного пространства: доступность информации (возможность за приемлемое время получить требуемую информационную услугу); целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения); конфиденциальность информации (защита от несанкционированного ознакомления).

Уровни информационной безопасности: законодательный (законы, нормативные акты, стандарты и т.п.); административный (действия общего характера, предпринимаемые руководством); процедурный (конкретные меры безопасности, имеющие дело с людьми); программно-технический (конкретные технические меры).

**Основные направления обеспечения информационной безопасности Российской Федерации.**

Место и роль информационной безопасности в обновленной концепции национальной безопасности РФ (2000). Основы национальной безопасности РФ в информационной сфере.

Доктрина информационной безопасности РФ: национальные интересы РФ в информационной сфере; объекты обеспечения информационной безопасности; внешние и внутренние угрозы национальной безопасности в информационной сфере; международное сотрудничество РФ в области обеспечения информационной безопасности.

Обзор законодательства РФ в области защиты информации.

Региональная информационная безопасность.

# ПЛАНЫ ИНТЕРАКТИВНЫХ ЛЕКЦИЙ-КОНСУЛЬТАЦИЙ

*Лекция-консультация №1*

**Информационное общество: теоретическая модель или реальность?**

1. Футурологические концепции постиндустриального (информационного) общества. Основные черты информационного общества (по работам Д. Белла, А. Тоффлера, М. Кастельса, Ф. Фукуямы и др.).

**Анализ результатов и последствий информационной революции.**

2. Информационная революция и «новая экономика».
3. Государство и власть, социальная структура, международные отношения в эпоху постиндустриализма.
4. Римский клуб об информационном обществе. Глобальная «инфосфера» как фактор трансформирующий современную цивилизацию.
5. «Информационная эпоха»: сбылись ли предсказания футурологов?

**Литература:**


1. Современная западная философия: Словарь/ Сост.: Малахов В.С., Филатов В.П. - М.: Политиздат, 1991. - 414 с.
2. Новая постиндустриальная волна на Западе. Антология/ Под ред. В.Л. Иноземцева. - М.: Academia, 1999.
3. В.Л. Иноземцев. Современное постиндустриальное общество. - М.: Логос, 2000.
4. Балуев Д.Г. Информационная революция и современные международные отношения: Уч. пособие. - Н.Новгород: ННГУ, 2001. - 107 с.
5. Введение в философию: Учебник для вузов. В 2 ч./ Под общ. Ред. И.Т. Фролова. - М.: Политиздат, 1989.
6. Гаджиев К.С. Введение в политическую науку: Учебник для вузов. - М.: Логос, 1999. - 544 с.
7. Тоффлер А. Третья волна. - М.: АСТ, 1999. - 748 с.
8. Белл Д. Грядущее постиндустриальное общество. - М.: Academia, 1999.
9. США 80-х: взгляд изнутри. «Американская модель»: с будущим в конфликте/ Под общ. ред. Г.Х. Шахназарова. - М.: Прогресс, 1984. - 256 с.
10. Римский клуб/ Сост. Д.А. Гвишиани, А.И. Колчин, Е.В. Нетесова, А.А. Сейтов. - М.: УРСС, 1997. - 384 с.
11. Компьютеризация общества и человеческий фактор. Реферативный сборник/ Отв. Ред. А.И. Ракитов. - М.: ИНИОН АН СССР, 1988. - 228 с.
12. Постиндустриальный мир: Центр, Периферия, Россия. Общие проблемы постиндустриальной эпохи. (Серия «Научные доклады», вып. 91.) - М.: МОНФ; ИМЭМО РАН, 1999. - 304с.
13. Постиндустриальный мир: Центр, Периферия, Россия. Особый случай России. (Серия «Научные доклады», вып. 93.) - М.: МОНФ; ИМЭМО РАН, 1999. - 224с.
14. Кеннеди П. Вступая в двадцать первый век. - М.: Весь Мир, 1997. - 480 с.
15. Братимов О.В., Горский Ю.М., Делягин М.Г., Коваленко А.А. Практика глобализации: игры и правила новой эпохи. - М.: ИНФРА-М, 2000. - 344 с.
16. Материалы сети Интернет по данной проблематике.


*Лекция-консультация №2*

**Опыт и проблемы становления глобального информационного общества.**

**Информационное «измерение» международной безопасности.**

1. Системный подход к проблемам безопасности. Изменение системных свойств современного мира, связанное с усложнением систем (примеры). Появление новых (системных) свойств у сложных систем (у целого появляются свойства, которыми не обладают части), с которыми связаны как новые ресурсы развития системы, так и новые источники угроз безопасности. Воздействие на информационную систему (сильное и слабое). Комплексный подход к обеспечению безопасности сложных систем.
2. Тенденция к усложнению мировой политической системы в процессе глобализации. Глобализация и международная безопасность. Возрастание роли невоенных составляющих безопасности. Информационная безопасность – важнейшая составляющая структуры международной безопасности.
3. «Реалистический» и «либеральный» подходы к проблеме информационной безопасности в современных международных отношениях.
4. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Обзор и характеристика новых видов угроз международной безопасности: распространение «метатехнологий»; электронно-цифровой разрыв; информатизационная милитаризация; компьютерная преступность и компьютерный терроризм.

**Современный мировой информационный порядок: правовые аспекты.**
**«Информационное общество» как политическая задача и международный проект. ИТ-проекты по развитию глобального информационного общества.**

5. Необходимость международно-правового регулирования процессов гражданской и военной информатизации. Резолюция ООН 54/49 и ее значение для мирового сообщества. Деятельность ООН в области регулирования информационной сферы.
6. Окинавская Хартия Глобального Информационного Общества: всесторонний анализ современной инфосферы, определение возможных путей международного сотрудничества в киберпространстве и попытка правового регулирования процесса глобальной информатизации. Деятельность G 7/8 в области регулирования информационной сферы.
7. Встреча на высшем уровне по вопросам информационного общества (ВВУИО – WSIS) как механизм регулирования и организации структур глобального информационного общества.
8. Другие международные (многосторонние и двусторонние) правовые акты в информационной сфере. Формирование международного информационного законодательства.

**Литература:**


1. Белянцев А.Е. Международная безопасность в условиях глобальной информационной революции//Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Международные отношения, Политология, Регионоведение. 2003. № 1. С. 311-320.
2. Окинавская Хартия Глобального Информационного Общества.
3. Документы ВВУИО – WSIS.
4. Почепцов Г.Г. Информационно-психологическая война. - М.: СИНТЕГ, 2000. - 180 с.
5. Расторгуев С.П. Философия информационной войны. - М.: Вузовская книга, 2001. - 468 с.
6. Балуев Д.Г. Завоевание будущего: внешняя политика России на рубеже веков: Монография. - Н.Новгород: ИСИ ННГУ,1999. - 122 с.
7. Балуев Д.Г. Информационная революция и современные международные отношения: Уч. пособие. - Н.Новгород: ННГУ, 2001. - 107 с.

8. Слипченко В.И. Война будущего. (Серия «Научные доклады», вып. 88.) - М.: МОНФ; Издательский центр научных и учебных программ, 1999. - 292с.
9. Модестов С.А. Информационное противоборство как фактор геополитической конкуренции. (Серия «Научные доклады», вып. 74.) - М.: МОНФ; Издательский центр научных и учебных программ, 1999. - 64с.
10. Политология. Учебник/ Отв. редактор В.М. Утенков. - М.: Редакционно-издательский центр МГОПУ, 2000. - 438 с.
11. Братимов О.В., Горский Ю.М., Делягин М.Г., Коваленко А.А. Практика глобализации: игры и правила новой эпохи. - М.: ИНФРА-М, 2000. - 344 с.
12. Запад: новые измерения национальной и международной безопасности: Монография. - Н.Новгород: ННГУ, 1997. - 348 с.
13. Международная конференция «Глобальные проблемы как источник чрезвычайных ситуаций» 22-23 апреля 1998 г. Доклады и выступления/ Под ред. Воробьева Ю.Л. - М.: УРСС, 1998. - 320 с.
14. Россия и НАТО после Балканского кризиса: Материалы международной научной конференции. - Н.Новгород: ННГУ, 2000. - 112 с.
15. Libicki, Martin C. What is information warfare? - Washington DC: NDU Press, 1995. - 104 p.
16. Libicki, Martin C. Defending cyberspace and other metaphors. - Washington DC: NDU Press, 1997. - 110 p.
17. Alberts, David S. Defencive information warfare. - Washington DC: NDU Press, 1996. - 82 p.
18. War in the information age: new challenges for US security policy/ edited by Robert L. Pfalzgraff, Jr, Richard Shultz, Jr. - Washington/London: Brassey's, 1997. - 376 p.
19. De Landa, Manuel. War in the age of intelligent machines. - New York: Swereve Editions, 1991. - 272 p.
20. Shukman, David. Tomorrow's war: the threat of high-technology weapons. - New York/San Diego/London: Hardcourt Brace&Company, 1996. - 272 p.
21. Van Creveld, Martin. Technology and war: from 2000 B.C. to the present. - New York: The Free Press. 1991. - 342 p.
22. Материалы сети Интернет по данной проблематике.

*Лекция-консультация №3*

**Информационная политика: мировой опыт.**

1. Информационная политика. Концептуальные принципы формирования информационной политики государства.
2. Национальные модели информационного общества и опыт их реализации. Сравнительный анализ информационной политики различных государств мира: опыт США, опыт стран Европейского сообщества, опыт Японии, опыт КНР, опыт стран Восточной Азии, опыт исламских государств и др. Уроки для России.

**Особенности современной информационной политики Российской Федерации.**

3. Социальные предпосылки и особенности становления информационного общества в России. Развитие в России информационной и коммуникационной инфраструктуры.
4. Государственная информационная политика России. Проблемы и перспективы интеграции России в мировое информационное общество.

**Литература:**

1. Балуев Д.Г. Завоевание будущего: внешняя политика России на рубеже веков: Монография. - Н.Новгород: ИСИ ННГУ,1999. - 122 с.
2. Балуев Д.Г. Информационная революция и современные международные отношения: Уч. пособие. - Н.Новгород: ННГУ, 2001. - 107 с.

3. Политология. Учебник/ Отв. редактор В.М. Утенков. - М.: Редакционно-издательский центр МГОПУ, 2000. - 438 с.
4. Компьютеризация общества и человеческий фактор. Реферативный сборник/ Отв. Ред. А.И. Ракитов. - М.: ИНИОН АН СССР, 1988. - 228 с.
5. Попов В.Д. Информационная политика. Учебник. – М.: РАГС. 2003. – 463 с.
6. Дайсон Э. Жизнь в эпоху Интернета. Release 2.0. - М.: Бизнес и Компьютер, 1998. - 400 с.
7. Libicki, Martin C. Defending cyberspace and other metaphors. - Washington DC: NDU Press, 1997. - 110 p.
8. Материалы сети Интернет по данной проблематике.

*Лекция-консультация №4*

**Политическая коммуникация в информационном обществе.**

1. Электронная демократия. Электронное правительство. Электронная (цифровая) дипломатия.
2. Понятие Интернет-СМИ, правовое регулирование и разновидности интернет-СМИ. Особенности ведения агитации в интернет-СМИ. История создания и развития интернет-СМИ в России. Блоги и «блогосфера».
3. Влияние новых информационных технологий на выборы. PR и реклама в информационном обществе.
4. Информационное управление: потенциальные возможности и опасности.
5. «Глобальное управление» в контексте информационной революции.

**Новые информационные технологии в политической практике.**

6. Технологии управления взаимоотношениями с населением (CRM). Геоинформационные технологии. WWW-технологии. Технологии аналитической обработки информации. Современные технологии совместной работы. Технологии построения и эксплуатации хранилищ информации. Технологии ситуационного управления.
7. Social software (управление сообществами через интернет).

**Компьютерные технологии в информационно–аналитической деятельности.**

8. Цели, задачи, объект, предмет, субъекты информационно-аналитической деятельности. Сущность и содержание информационно-аналитической деятельности.
9. Методы анализа, связанные с использованием новых информационных технологий. Сбор информации с использованием сети Интернет. Роль информации, собираемой из открытых источников.

**Литература:**

9. Балуев Д.Г. Информационная революция и современные международные отношения: Уч. пособие. - Н.Новгород: ННГУ, 2001. - 107 с.
10. Политология. Учебник/ Отв. редактор В.М. Утенков. - М.: Редакционно-издательский центр МГОПУ, 2000. - 438 с.
11. Компьютеризация общества и человеческий фактор. Реферативный сборник/ Отв. Ред. А.И. Ракитов. - М.: ИНИОН АН СССР, 1988. - 228 с.
12. Попов В.Д. Информационная политика. Учебник. – М.: РАГС. 2003. – 463 с.
13. Поппель Г., Голдстайн Г. Информационная технология - миллионные прибыли. - М.: Экономика, 1990. - 238 с.
14. Васкевич Д. Стратегии клиент/сервер. Руководство по выживанию для специалистов по реорганизации бизнеса. - К.: Диалектика, 1996. - 384 с.
15. Дайсон Э. Жизнь в эпоху Интернета. Release 2.0. - М.: Бизнес и Компьютер, 1998. - 400 с.

16. Международная конференция «Глобальные проблемы как источник чрезвычайных ситуаций» 22-23 апреля 1998 г. Доклады и выступления/ Под ред. Воробьева Ю.Л. - М.: УРСС, 1998. - 320 с.
17. Материалы сети Интернет по данной проблематике.

# ПРИМЕРНАЯ ТЕМАТИКА ТВОРЧЕСКИХ ПИСЬМЕННЫХ РАБОТ

***Темы рефератов***

*1. Теоретические основания концепции информационного общества*

1. Построение концептуальных и прогностических моделей общественного развития в западной социологии – [на примере: постиндустриальное общество, общество постмодерна, сетевое общество, глобальное общество, информационное общество].
2. «Постиндустриальное общество» в трактовке Д.Белла.
3. О. Тоффлер о социальных изменениях – трилогия «Шок будущего», «Третья волна», «Метаморфозы власти».
4. «Между двух веков. Роль Америки в технотронную эру» З. Бзежинского - лидерство в информационном обществе – лидерство в новом мировом порядке.
5. «Информационная революция и политика: оправдались ли ожидания?» (на основе анализа ТЕКСТОВ Д.Белла, О.Тоффлера, З. Бзежинского, М.Маклюэна, М.Кастельса, П.Норрис и др. (по выбору студента) и современных тенденций развития).
6. «Конфликты и противоречия информационной цивилизации» (на основе анализа ТЕКСТОВ Д.Белла, О.Тоффлера, З.Бзежинского, М.Маклюэна и др. (по выбору студента) и современных тенденций развития).
7. Когнитариат, меритократия, нетократия – кому принадлежит власть в новом обществе?
8. Трансформация труда и занятости: сетевые работники, безработные и работники с гибким рабочим днем.
9. Повседневная жизнь в электронном коттедже: конец городов? Трансформация городской формы: информациональный город?
10. Изменение «пространства» и «времени» в постиндустриальном обществе. Размывание жизненного цикла: на пути к социальной аритмии.
11. Информациональный капитализм Мануэля Кастельса.
12. Плоский мир Томаса Фридмана.
13. «Старший брат» или «маленькие сестры». Политическая воля или культурная революция – что эффективнее?
14. «Фабрики мысли». Корпорация РЭНД (RAND). Исследования и прогнозы в области науки и развития технологий.

*2. «Информационное общество» как политическая задача и международный проект. Международные организации – повестка дня…*

1. Свобода выражения и безопасность в Интернете (Freedom of expression and security on the Internet ) в повестке дня международных неправительственных организаций.
2. Общая организационная структура существующих механизмов управления Интернетом.
3. Международные переговоры по управлению интернетом. Дискуссия вокруг ICANN.
4. "Цифровой разрыв", проблема универсального доступа к инфраструктуре ИКТ для всех в повестке дня международных неправительственных организаций.
5. Разнообразие, многоязычие, поощрение и защита локального контента в повестке дня международных неправительственных организаций.
6. Интернационализированные доменные имена в повестке дня международных неправительственных организаций.
7. Проблема кибертерроризма в повестке дня международных неправительственных организаций.
8. Проблема киберэкстремизма в повестке дня международных неправительственных организаций.
9. Динамика вопросов повестки дня международных неправительственных организаций. 1997 -2008.

10. Цели и позиция России в участии в международных институтах по развитию глобального информационного общества.

*3. Россия в мировом информационном пространстве*

1 Россия в мировом информационном пространстве: объективные показатели: развитие и доступ к ИКТ, образование, «новая экономика», общество и ИТ.
2 Россия в мировом информационном пространстве: политические задачи. «Электронная Россия».
3 Позиция России в международных программах реализации информационного общества.
4 Успехи и неудачи инновационной политики России.
5 Опыт межстрановых сопоставлений и возможности заимствований отдельных мероприятий и стратегии инновационной политики.
6 Институциональные условия формирования инновационной политики в РФ пореформенного периода.
7 Эффективность прямых и косвенных методов поддержки инновационной деятельности в РФ. Особые зоны: [по выбору студента - наукограды, региональные кластеры; Мегапроекты, VIP-проекты, частно - государственное партнёрство; Венчурные фонды, Российская венчурная корпорация; Фонды целевого капитала (endowment)].
8 Стратегии технологического развития развитых стран Связь технологий, инноваций и организационной структуры.
9 Стратегии инновационного развития новых индустриальных стран. Потенциал технологического самообучения. Кристаллы технологического развития и возможности перехода от пассивных к активным стратегиям.

*4 Россия в мировом информационном пространстве: политические задачи. «Электронная Россия».*

1 Административная реформа и «Электронное государство» в России: возможности интеграции.
2 Многофункциональные центры («супермаркеты госуслуг») – идеология, архитектура, административные регламенты.
3 Создание специализированного портала госуслуг: идеология, архитектура, административные регламенты.
4 Методы мониторинга и оценки эффективности электронной государственной услуги. Продвижение электронных государственных услуг для бизнеса.
5 Мобильная демократия – от пилотных проектов к массовому внедрению.
6 Региональная информационная политика и кластерный подход к развитию инноваций в сфере ИКТ, малого и среднего бизнеса.
7 ИКТ в национальных проектах - 2008. Стратегические вопросы.
8 ИКТ в национальных проектах- 2008. ИТ в здравоохранении – международный опыт и развитие здравоохранения в России.
9 ИКТ в национальных проектах- 2008. ИКТ в образовании – международный опыт и развитие в России.
10 ИКТ в национальных проектах- 2008. ИТ в ЖКХ – опыт и возможности.
11 ИКТ в национальных проектах – 2008. ИТ в АПК – опыт и возможности.
12 Развитие ИКТ, «новой экономики» и высокотехнологичных отраслей как условия стратегического развития России в политической повестке дня – 2008 [в программах политических партий и лидеров, в предвыборной борьбе – по выбору студента]

***Примерные темы исследований и эссе***

1. Особенности формирования образа политика в Интернет (на основе анализа персональных страниц политических лидеров).
2. Анализ политических предпочтений аудитории российского Интернета (по материалам

социологических исследований ФОМ, ФЭП, КОМКОН-2, РОЦИТ и др.)
3. Составление списка аннотированных Интернет-ресурсов по отдельным проблемам политической науки.
4. Проведение небольшого эмпирического исследования (4-5 интервью) на тему «Политические новости: ТВ или Интернет?» Составление отчета (до 5 стр.)
5. Эссе «Дилемма «Свобода» – «Регулирование» в информационном пространстве» на основе анализа статей Пауля.Треанора «Интернет как гиперлиберализм» и Джона Перри Барлоу «Декларация независимости киберпространства» (3-5 стр.)
6. Эссе «Информационная революция и политика: оправдались ли ожидания?» (на основе анализа представлений теоретиков постиндустриального развития Д.Белла, О.Тоффлера, З.Бзежинского, М.Маклюэна и др. (по выбору студента) и современных тенденций развития) – 5-10 стр.
7. Эссе «Конфликты и противоречия информационной цивилизации» (на основе анализа представлений теоретиков постиндустриального развития Д.Белла, О.Тоффлера, З.Бзежинского, М.Маклюэна и др. (по выбору студента) и современных тенденций развития) – 5-10 стр.
8. Эссе «Идеология Интернет – между коммуникационной утопией и технократическим мифом».

**Источник:**
http://www.umk.utmn.ru/?section=discipline&spy_id=703&d_id=23936&dh_id=31396&specialize_id=#ekz
(08.10.2011)

# МАТЕРИАЛЫ ДЛЯ ПОДГОТОВКИ К ИНФОРМАТИВНЫМ ЛЕКЦИЯМ И К ИНТЕРАКТИВНЫМ ЛЕКЦИЯМ-КОНСУЛЬТАЦИЯМ

*ГРАЧЕВ М.Н.*

## ПОЛИТИЧЕСКАЯ КОММУНИКАЦИЯ

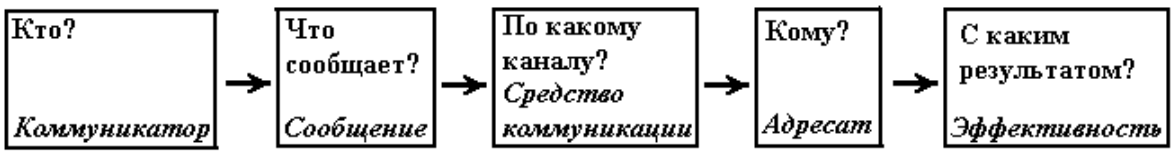
### 1. Понятие политической коммуникации

Политика не существует вне человеческой деятельности, различных способов взаимодействия ее носителей, вне коммуникационных процессов, связывающих, направляющих и инновациирующих общественно-политическую жизнь. Политическая коммуникация выступает своеобразным социально-информационным полем политики. Ее роль в политической жизни общества сопоставима, по образному выражению французского политолога Ж.-М. Коттрэ, со значением кровообращения для организма человека[1]. Политическая коммуникация представляет собой совокупность процессов информационного обмена, передачи политической информации, структурирующих политическую деятельность и придающих ей новое значение.

Началом изучения явлений политической коммуникации в развитых странах можно считать исследования пропаганды в период первой мировой войны. Однако фундаментальные работы в этой области, равно как и сам термин “политическая коммуникация”, появились лишь в конце 40-х – начале 50-х годов. Выделение исследований политической коммуникации в самостоятельное направление, связанное с использованием формализованных методов системного анализа, приходится на 50-е – 60-е годы – период становления общей теории систем как междисциплинарной логико-методологической концепции исследования сложноструктурированных объектов различной природы, а также стремительного развития кибернетики – области знания, изучающей наиболее общие закономерности процессов информационного обмена и управления в технических, биологических, человеко-машинных, экономических и социальных системах.

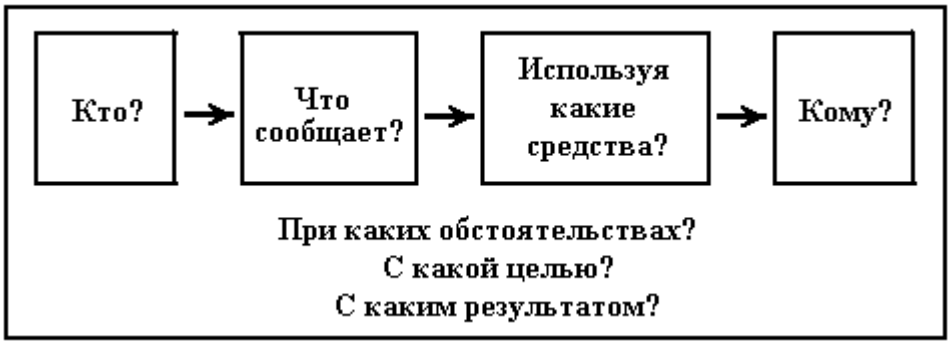
Полвека назад американский политолог Г.Лассуэлл начал свою знаменитую статью, положившую начало исследованиям политической коммуникации, с логической схемы: “Наиболее подходящий способ описания коммуникационного акта состоит в том, чтобы ответить на следующие вопросы: Кто? Что сообщает? По какому каналу? Кому? С каким результатом?”[11]

Впоследствии данная конструкция получила название формулы Лассуэлла. Ее графическая интерпретация показана на рис.




В дальнейшем эта несложная схема обычно применялась в качестве иллюстрации круга основных проблем, находящихся в поле зрения коммуникационных исследований. Однако многие исследователи, не отрицая определенной практической пользы формулы Лассуэлла, справедливо отмечали, что она, является упрощением. Некоторые из них предлагали усовершенствовать эту модель, дополнив ее новыми компонентами. Так, по мнению Р. Брэддока, описание коммуникационного процесса должно включать еще два принципиально важных момента: при каких обстоятельствах и с какой целью направляется

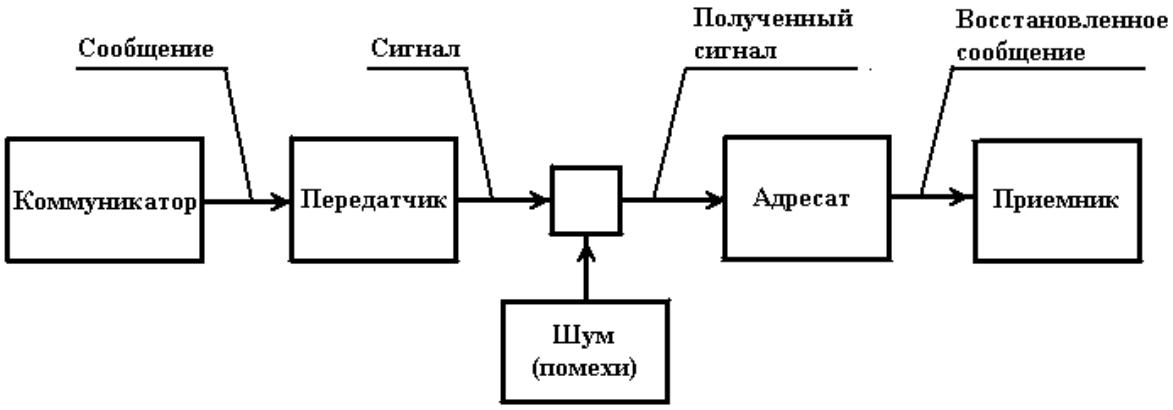
данное сообщение[12]. Предложенный Р. Брэддоком вариант “расширения” формулы Лассуэлла показан на рис.




Формула Лассуэлла трактует политическую коммуникацию преимущественно как императивный, побудительный процесс: “отправитель” в той или иной степени стремится оказать влияние на “адресата”. Между тем ей присуще одно далеко не бесспорное допущение, которое заключается в том, что передаваемые сообщения всегда вызывают определенный ожидаемый эффект. Эта модель, несомненно, имеет тенденцию преувеличивать результативность воздействия передаваемых сообщений, особенно когда речь идет о средствах массовой коммуникации.

На разработку ранних моделей коммуникационных процессов оказали заметное влияние идеи Клода Шеннона, известного математика и одного из основоположников теории информации. В конце 40-х годов, будучи сотрудником знаменитой лаборатории “Белл Телефон”, он занимался решением прикладных инженерно-технических задач, связанных с проблемами передачи информации по различным каналам связи. Тем не менее, графическая интерпретация коммуникационного процесса, предложенная К. Шенноном и его коллегой У. Уивером применительно к вопросам технико-технологического характера[13], практически сразу привлекла внимание политологов и специалистов в области средств массовой информации.

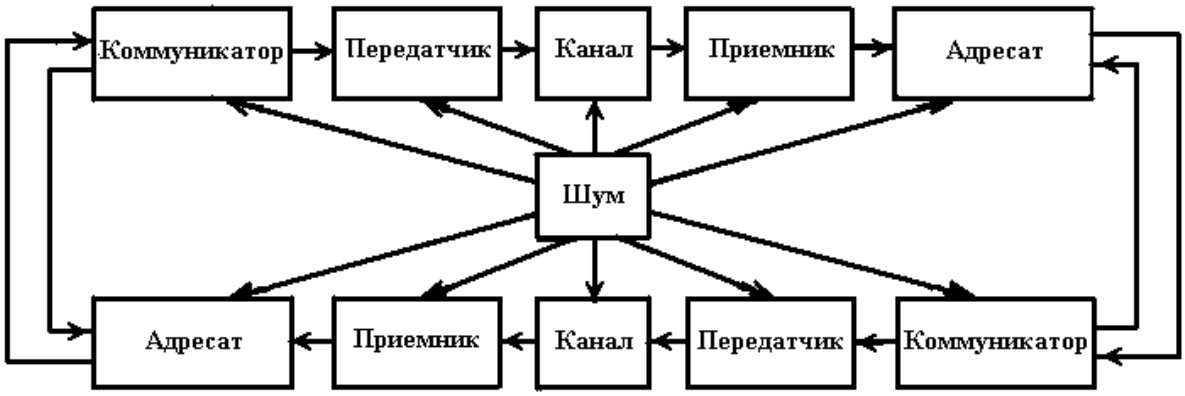
Модель Шеннона – Уивера описывает коммуникацию как линейный и однонаправленный процесс . Вначале *источник информации* создает *сообщение* (в более общем случае – последовательность сообщений), которое затем поступает в *передатчик*, где принимает форму *сигнала*, адаптированного для передачи по каналу связи, ведущему к *приемнику*. Приемник восстанавливает сообщение из *полученного сигнала*. Затем *восстановленное сообщение* достигает *адресата*. В процессе передачи сигнал обычно искажается *шумом*, или *помехами*, которые возникают, например, при одновременной передаче нескольких сообщений по одному каналу. Наложение помех приводит к тому, что переданный и полученный сигнал будут в большей или меньшей степени отличаться друг от друга. Соответственно, сообщение, созданное источником информации, и сообщение, которое получил адресат как сигнал, восстановленный приемником, так или иначе будут иметь разное содержание, вплоть до того, что иногда они даже могут не совпадать в смысловом отношении.




В отличие от формулы Лассуэлла, модель Шеннона – Уивера оказывается значительно ближе к действительности. Она наглядно демонстрирует, что передаваемые по каналам связи сообщения отнюдь не всегда приводят к ожидаемому результату.Однако здесь так же, как и в формуле Лассуэлла, отсутствуют принципиально важные для властно-управленческих отношений элементы обратной связи. В результате процесс управления предстает лишь как единичный и далеко не всегда эффективный акт: “источник информации” не имеет возможности контролировать действия “адресата” и, соответственно, корректировать свои последующие управляющие воздействия таким образом, чтобы поведение “управляемого” все более и более приближалось к заданному.

В 1970 г. М.Дефлёр предложил существенно видоизменить модель Шеннона – Уивера. Новая интерпретация коммуникационного процесса выдвигает на первый план проблему соотношения двух смысловых значений – первоначального сообщения, отправленного “источником”, и восстановленного сообщения, поступающего к “управляемому адресату”. При этом сам термин “коммуникация” понимается как результат достижения соответствия между исходным и конечным “значениями”[14].

По сравнению с исходной моделью, схема коммуникационного процесса дополнена петлей обратной связи. Коммуникация, как следует из концепции М.Дефлёра, начинается с того, что *источник*, выступающий инициатором коммуникационного акта, формулирует некоторое смысловое “значение” в виде “сообщения”, которое направляется в *передатчик*, где оно, соответственно, преобразуется в “информацию”, адаптированную для передачи по каналам связи. В свою очередь, “информация” проходит через какой-либо *канал* (в роли канала, в частности, могут выступать и *средства массовой информации*) и поступает в *приемник*, где происходит расшифровка “информации”: она превращается в “сообщение”, которое затем преобразуется “управляемым” *адресатом* в “значение”.




Проблема возможного несоответствия между исходным и восстановленным “значениями” решается в модели Дефлёра путем использования линии обратной связи, включающей в себя такую же последовательность компонентов. *Источник*, имеющий непосредственную связь с “управляемым” адресатом, формулирует о нем содержащее

определенную смысловую нагрузку “сообщение”, которое поступает в *передатчик* и преобразуется в “информацию”. По *каналу обратной связи* “информация” поступает в *приемник*, где из нее восстанавливается “сообщение”, которое получает *адресат*, имеющий двухстороннюю связь с инициатором коммуникационного акта. В результате инициатор получает возможность контролировать и при необходимости корректировать ход коммуникационного процесса, увеличивая тем самым вероятность достижения соответствия между “значениями” двух “сообщений” – исходного и поступающего к “управляемому” адресату.

Таким образом, развитие М. Дефлёром идей К. Шеннона и У. Уивера, позволяет преодолеть очевидные недостатки исходной модели – линейность, однонаправленность и отсутствие обратной связи. Однако, как нетрудно заметить, и здесь в центре внимания оказывается прежде всего проблема промежуточных преобразований и неизбежных искажений передаваемого “сообщения”. При этом функции “инициатора коммуникации”, только формулирующего некоторое “смысловое значение” в виде передаваемого “сообщения”, и “управляемого адресата”, только восстанавливающего это “значение” из принятого “сообщения”, оказываются жестко зафиксированными и четко разграниченными.

При исследовании эволюции способов политической коммуникации основной акцент делается на анализ отношений управляющих и управляемых в коммуникативном плане. Ж.-М.Коттрэ предложил рассматривать их в следующей парадигме:

1. Отношения идентичности. Управляющие идентичны управляемым.

2. Отношения включения. Все управляющие являются членами политического общества, но не все управляемые являются членами руководящего круга. Эти отношения заключают в себе взаимопроникновение и взаимовлияние управляющих и управляемых.

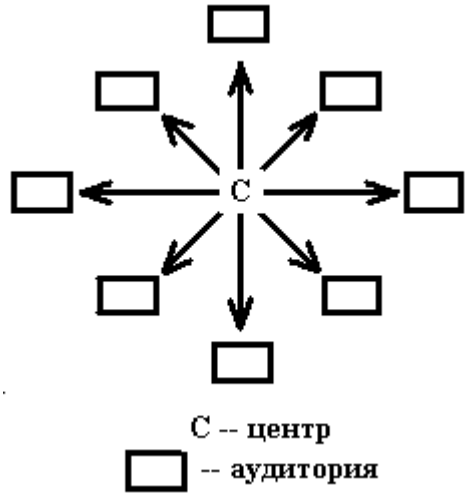
3. В условиях расширения политического общества отношения между управляющими и управляемыми становятся отношениями пересечения. Класс управляющих частично отделяется от класса управляемых[15].


В ряде моделей политической коммуникации обращается внимание на роль элиты, которая осуществляет свою власть над остальной частью общества не непосредственно, а через промежуточные звенья – бюрократический аппарат и СМК. На рис. приводится модель К.Сайнне, в которой показывается, что между такими элементами политической системы, как элита, бюрократия и массы, происходит непрерывный информационный обмен, причем элиты всегда конструируют и передают “вниз” информацию, которая бы укрепляла их собственную легитимность[16].

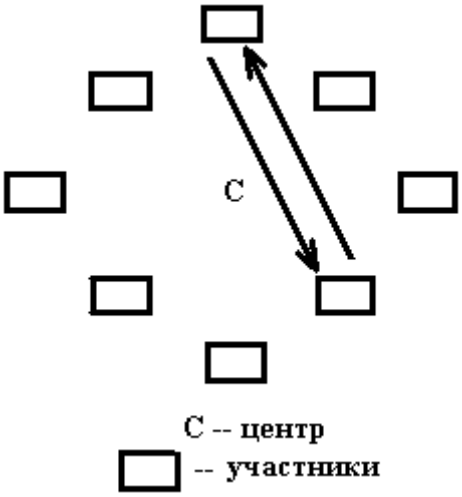

Действительно, субъекты массовой коммуникации господствующего социального слоя, класса обычно занимают ведущее положение в обществе и имеют наиболее благоприятные условия для информационно-пропагандистской деятельности. “Господствующими идеями любого времени, – как верно отмечали К.Маркс и Ф.Энгельс, – были всегда лишь идеи господствующего класса”[17]. Понятно, что такой класс, направляя деятельность государственных институтов, стремится контролировать основные средства коммуникации, идеологические учреждения и т.д. В зависимости от уровня политической культуры общества он это делает демократическими или авторитарными способами, единолично или с союзниками, с учетом мнения и настроений масс или же без такового. Л.С.Санистебан обращал внимание на то, что “общественное мнение формируется прежде всего под влиянием средств массовой информации, и, конечно, политические элиты пытаются сделать так, чтобы общественное мнение или, по крайней мере, преобладающая его часть склонялось в их пользу[18].

Вместе с тем было бы неверно анализировать коммуникационные отношения только по вертикальному принципу: “правящие элиты – управляемые массы”. Чем демократичнее общество, тем большее значение приобретает горизонтальный уровень обмена потоками политической информации, сопряжение господствующего коммуникационного потока, инициируемого государством, с информационными потребностями и приоритетами гражданского общества, формирующимися на более широкой ценностной основе. Кроме того, следует учитывать и влияние новых электронных средств связи, которые делают привычным набор услуг телекоммуникационной сети, позволяющей своим пользователям более свободно отправлять и принимать информацию как личного, так и общественного характера. Так, персональный компьютер, сопряженный при помощи специальных устройств – модемов с телефонной сетью, позволяет индивидам не только общаться друг с другом, но и получать в зависимости от их желания или потребностей необходимую информацию из какого-либо банка данных. Наряду с этим использование электронной почты, телефакса, мобильных телефонов и других новейших средств, со всей очевидностью, способствуют усилению межличностного взаимодействия.

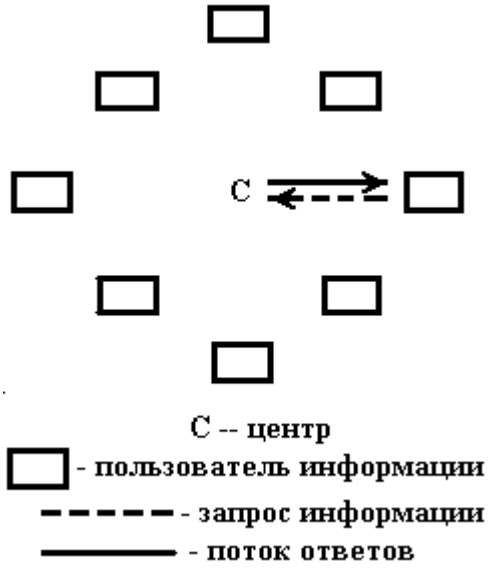
Сущность изменений в области политической коммуникации, которые позволяют (по крайней мере, в принципе) преодолеть доминирование и жесткий контроль отправителя информации над адресатом, достаточно наглядно иллюстрируется при помощи моделей альтернативных видов движения информации, предложенных голландскими исследователями Й. Бордвиком и Б. ван Каамом[19].



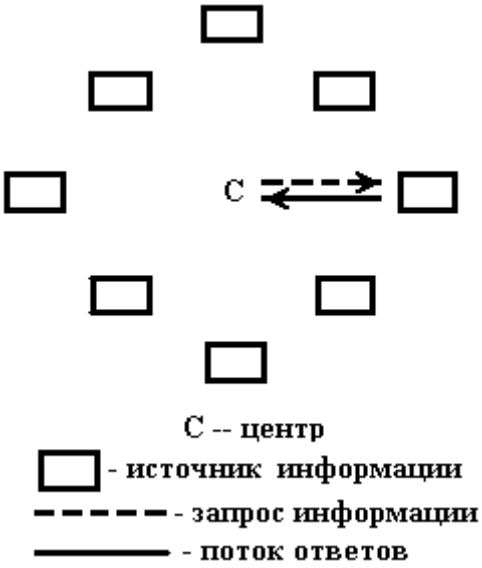

*1)*




*2)*




*3)*




*4)*

1. *Модель вещания* предполагает распространение информации из центра одновременно многим абонентам на периферии. Эта ситуация встречается достаточно часто: например, во время лекции или официального доклада, когда слушатели сосредоточены в какой-либо аудитории, а также в случае телерадиопередачи, когда некоторое сообщение одновременно принимается достаточно большим количеством людей, находящихся в разных местах. Характерными чертами данной модели как типичной односторонней коммуникации являются относительно малая возможность личной обратной связи (особенно, если речь идет о СМИ), а также то обстоятельство, что время и место коммуникации определено отправителем.

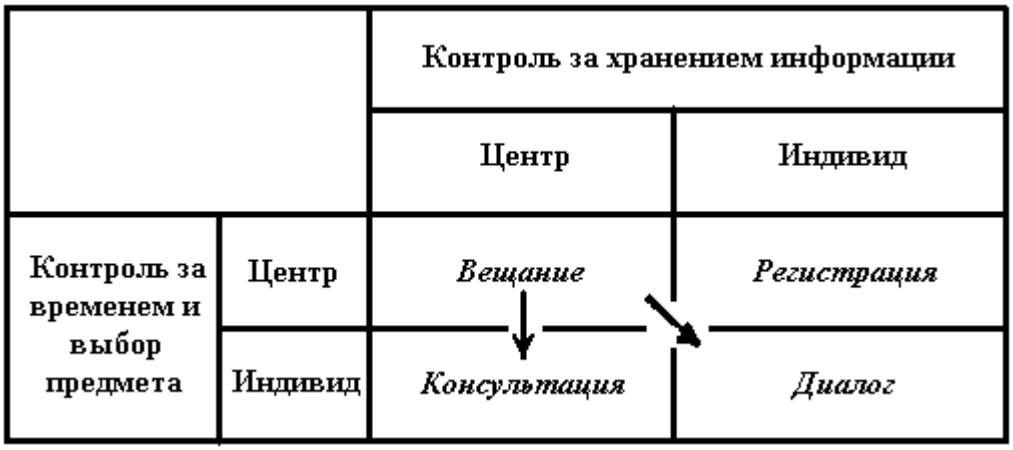
2. *Диалоговая модель* относится к случаю распространения информации в реальной коммуникационной сети: индивиды общаются непосредственно между собой, игнорируя центр или посредников и самостоятельно выбирая время, место и тему информационного обмена. Эта модель также имеет широкий круг применения: от простой личной переписки и телефонных переговоров до использования “Интернета” и электронной почты. Характерное отличие диалоговой модели состоит в том, что она предполагает своеобразное “горизонтальное равенство” участников информационного обмена, в противоположность “вертикальному” принципу “руководства – подчинения”, присущему модели вещания. Несомненно, коммуникация подобного вида не исключает участия и более двух сторон

(например, небольшая встреча, телефонная конференция, дискуссия на сайте сети “Интернет” и т. д.). Однако увеличение количества участников и, в частности, появление “ведущего” приводит к сближению данной модели с моделью вещания.

3. *Консультационная модель* также соотносится с большим числом ситуаций, при которых индивид, находящийся на периферии коммуникационной линии, ищет необходимые сведения в центральном информационном хранилище (сервер или иной банк данных, в наиболее простом варианте – работа с книгами, газетами и иной печатной продукцией в библиотеке). В отличие от модели вещания здесь место и время консультации, а также тема сообщения определяются не центром, а периферийным пользователем, обладающим максимальной свободой.

4. *Регистрационная модель* движения информации (рис. 14*г*) является противоположностью консультационной модели. В ней центр запрашивает и получает информацию от периферийного источника. Данная модель применяется, например, в случае, когда индивиду закрыт доступ к центральному банку данных, а также при автоматической записи телефонных сообщений, во всех системах электронной сигнализации и наблюдения. При этом сосредоточение информации в центре нередко происходит помимо желания индивида или без согласования с ним. Хотя данная схема исторически не нова, ее возможности значительно возросли вследствие **[с.34]** компьютеризации и расширения телекоммуникационных сетей. Типичным для регистрационной модели является то обстоятельство, что центр имеет больший контроль над определением направления информационного потока, чем находящийся на периферии коммуникационной сети индивид.

Приведенные модели информационных потоков не так резко отличаются друг от друга, как это могло бы показаться на первый взгляд, и на практике они отчасти перекрывают и взаимодополняют друг друга. К тому же существующая сегодня технология (например, телекоммуникационная инфраструктура) может обеспечить пользователя инструментарием для каждой из этих четырех моделей. Й.Бордвик и Б. ван Каам показали их логическую взаимосвязь, избрав в качестве критериев характер контроля как за хранением информации, так и за выбором времени и предмета сообщения (см. рис. 15). Стрелки графика показывают перераспределение движения информации от модели вещания к диалоговой и консультационной моделям. В общем плане это подразумевает изменение баланса коммуникативного потока от отправителя к адресату, что, однако, может быть уравновешено увеличением потока регистрации и новыми формами вещания, которое не утрачивает своих нынешних объемов, а все больше ориентируется на удовлетворение специфических интересов и потребностей сравнительно небольших аудиторий (например, кабельное телевидение).




**2. Проблемы политической коммуникации в постиндустриальном обществе**

Развитие новых технологий передачи и обработки информации, возрастание роли “четвертичного”, информационного сектора экономики, который следует за сельским

хозяйством, промышленностью и сферой услуг, пронизывая своим влиянием все области социальной действительности и по-новому организуя общественные отношения, позволяет, как подчеркнул несколько лет назад Д.Белл, говорить о том, что “постиндустриальное общество – это не проекция и не экстраполяция уже существующих в западном обществе тенденций развития, а новый принцип социально-технической организации жизни, точно такой же, как индустриальная система, заменившая собой аграрную”[20]. Реальной основой социально-философских теорий постиндустриализма служит происшедшая в 60-е – 70-е гг. в ряде развитых стран структурная перестройка хозяйственного механизма, выдвинувшая на первые позиции новые наукоемкие отрасли взамен тяжелой промышленности и сопровождавшаяся бурным развитием “индустрии знаний”, глобальной компьютеризацией и появлением разветвленных информационных систем, открывающих путь к децентрализации производства, его переориентации от погони за чисто количественным ростом в сторону улучшения “качества жизни”, существенного расширения сферы внеэкономических социальных программ.

Современный этап исследования проблем постиндустриального развития характеризуется разработкой концепции “информационного общества”. Еще в 50-е годы Н. Винер справедливо предсказывал, что в будущем “развитию обмена информацией между человеком и машиной, между машиной и человеком и между машиной и машиной суждено играть все возрастающую роль”[21]. В научный оборот понятие “информационного общества” было введено в 1981 г. японским ученым И.Ито[22]. В дальнейшем эта концепция получила свое дальнейшее развитие в работах Д. Белла, З. Бжезинского, Р. Дарендорфа, А. Кинга, И. Масуды, Дж. Нэйсбитта, О. Тоффлера, А. Шаффа и ряда других видных зарубежных исследователей[23].

По словам руководителя кафедры информационных исследований Королевского университета в Белфасте, директора Центра информационного менеджмента У. Мартина, под информационным обществом понимается “развитое индустриальное общество”, утверждающееся в Японии, США и Западной Европе, отличительными характеристиками которого являются следующие критерии:

– технологический: ключевой фактор – информационная технология, которая широко применяется на производстве, в учреждениях, системе образования и в быту;

– социальный: информация выступает как важный стимулятор изменения качества жизни, формируется и утверждается “информационное сознание” при широком доступе к информации;

– экономический: информация составляет ключевой фактор экономики в качестве ресурса, услуг, товара, источника добавленной стоимости и занятости;

– политический: свобода информации, ведущая к политическому процессу, который отличается растущим участием и консенсусом между различными классами и социальными слоями населения;

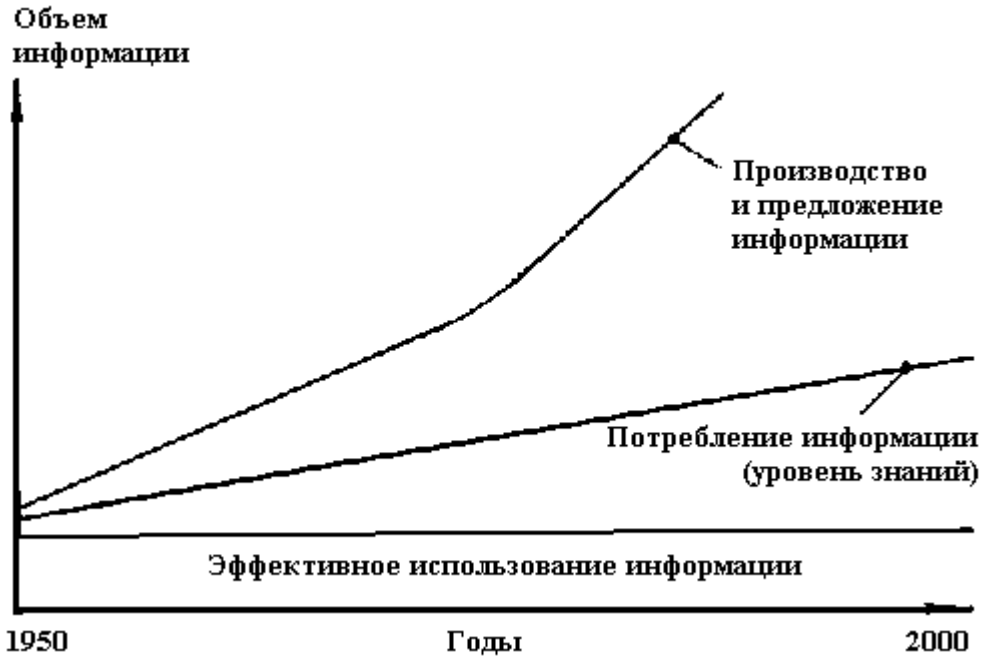
– культурный: признание культурной ценности информации, содействие утверждению информационных ценностей в интересах развития отдельного индивида и общества в целом[24].

В информационном обществе, по мнению У.Мартина, “качество жизни, так же как перспективы социальных изменений и экономического развития, в возрастающей степени зависят от информации и ее использования. В таком обществе стандарты жизни, формы труда и отдыха, система образования и рынок находятся под значительным влиянием достижений в сфере информации и знания”. Вместе с тем, отмечая позитивное влияние новых информационных технологий, исследователь одновременно обращает внимание на то, что они содержат и немалые возможности для нарушения принципов демократического устройства общества, прав и свобод человека. Это может выразиться не только, например, в создании “электронной картотеки” на каждого жителя страны, но и в отсутствии свободного доступа к информации простых граждан, нередко вынужденных довольствоваться сведениями, которые носят отрывочный характер или же тенденциозно подобраны

соответствующими службами, тем более что во многих государствах “пока не приняты законы о свободе информации”[25].

Конечно же, современный мир далек от модели “постиндустриального тоталитаризма” в духе антиутопий Дж. Оруэлла и А. Хаксли. Более того, развитие вычислительной техники, средств информатики и систем телекоммуникации резко расширило возможности индивидуального общения и неконтролируемого восприятия информации, поставив под сомнение саму возможность существования тоталитарных режимов в развитых странах. “На нашей планете, – отмечают Дж. Нэйсбитт и П. Абурден, – сегодня меньше диктаторов потому, что они уже не способны контролировать информацию”[26]. Действительно, контроль и распространение сведений политического характера – важный элемент в определении типа политических режимов: при авторитаризме информационные процессы берутся под строгий контроль, тогда как демократический режим предполагает, что политическая информация широко распространяется между различными членами общества. В основе идеальной, подлинно демократической модели политической коммуникации лежит диалог между “управляющими” и “управляемыми”, предполагающий равноправный обмен точными, полными, завершенными и проверяемыми сведениями о политических явлениях и процессах, сопрягаемыми с основными цивилизационно-культурными ценностями данного общества, фундаментальными правами и свободами личности. Особое значение при этом имеют свобода политических, религиозных и иных убеждений, свобода совести, свобода слова и печати, митингов и собраний, свобода объединений, а также право беспрепятственно придерживаться и свободно выражать свое мнение, свободно искать, получать и распространять всякого рода информацию и идеи независимо от государственных границ, если они не противоречат гуманистическим принципам. Интеллектуальная свобода, наличие просвещенного общественного мнения, демократическая политическая культура, свобода средств массовой информации от властных структур – важные предпосылки оптимального развития политической коммуникации, устойчивого социального процесса. В этом смысле теория политической коммуникации должна все в большей степени выступать, как наука и искусство достижения гармонии, координации интересов общества, его групп и индивидов посредством взаимопонимания, основанного на правде и полной информированности, уважении коренных интересов человека.

Сегодня пока еще не ясно, будет ли информационное общество “более информированным”. Дело в том, что в результате научно-технической революции себестоимость производства и передачи единицы информации существенно сократилась, однако при этом способность производить информацию намного превысила человеческие способности по ее переработке. Как показал голландский исследователь Й. ван Квиленбург, производство и предложение информации ежегодно возрастает на 8-10%, тогда как ее потребление растет значительно медленнее, а наблюдаемый положительный эффект кажется более или менее постоянным, хотя, конечно, его гораздо сложнее измерить . Данная ситуация “информационного перепроизводства”, нарушения баланса между “спросом” и “предложением” сопоставима, по мнению Й. ван Квиленбурга, с действием артиллерийского снаряда, который попал в цель, но не взорвался, ибо, с точки зрения пользователя, возникшая перегрузка прежде всего значительно усложнила поиск необходимых сведений, и данном случае мы наблюдаем эффект убывающей отдачи отдачи[27]. В этих условиях все большее внимание уделяется разработке и использованию консультирующих экспертных систем “искусственного интеллекта”, выступающих в роли “надежного советчика” человека при принятии решений в самых разных областях, в том числе и в политике.




Проблема, однако, состоит в том, что на заложенные в программное обеспечение "электронного эксперта" человеческие способы логического вывода накладываются совершенно нечеловеческие мощности в скорости действия и переборе вариантов, и в результате такой комбинации параметров компьютера предлагаемая им рекомендация нередко становится непонятной для пользователя. Конечно, разработчики подобных консультационных систем максимально позаботились о том, чтобы преодолеть эту ситуацию, разработав подсистему объяснения, которая по требованию пользователя может шаг за шагом растолковывать ему, как был получен предложенный вывод. Тем не менее, и такая процедура очень часто вызывает даже у подготовленного специалиста чувство недоумения и снижения самооценки, вызванного по крайней мере двумя причинами: разницей в уровне его собственных знаний и компетентности эксперта, послужившего прототипом для компьютерной базы данных, а также значительной длиной цепочки рассуждений, осуществленных системой. Еще сложнее обстоит дело с пониманием логики работы "электронных консультантов", построенных по принципу так называемых самообучающихся интеллектуальных систем, способных не только оперировать сведениями из различных банков и баз данных, но и учитывать в процессе своей работы стиль деятельности пользователя, что в перспективе вовсе не исключает "игры" на его сильных и слабых сторонах, подобно тому, как это отнюдь не безуспешно делают современные шахматные компьютеры.

Указанные особенности консультационных компьютерных систем могут, очевидно, привести к трем стратегиям поведения пользователя, из которых ни одна нельзя назвать оптимальным. Первый случай, когда пользователь продолжает предпринимать усилия в освоении системы и постижении логики ее работы путем своеобразного "соперничества интеллектов", приводит к психологическому перенапряжению и растрате сил специалиста. Не менее негативные последствия способен вызвать и второй вариант, когда пользователь отказывается от помощи "электронного консультанта", будучи не в состоянии "справиться" с ним. И, наконец, третья ситуация, когда пользователь полностью доверяет системе и действует исключительно в соответствии с ее рекомендациями, как бы полностью подчиняясь "искусственному интеллекту", может в отдаленной перспективе привести к технократическому самоуничтожению человечества[28].

Позитивное решение данной проблемы состоит, на наш взгляд, в отказе от самоценности техники и в опоре на гуманистические традиции, на культуру.

Принципиальное значение имеет ценностное измерение политической коммуникации, ее основных потоков, их целей и направленности. Известный специалист в области теории информации Д. Маккуэйл полагает, что культурная политика в области политической коммуникации должна основываться на таких принципах, как приоритетность качеств и ценностей данной культуры (иерархия); равные права и широкие возможности для приобщения к информации вследствие утверждения справедливости, демократии и широких прав граждан (равенство); близость к культуре нации, этнической общности или религиозного большинства (идентичность); учет моральных норм и требований (вкус и мораль)[29].

Ценностные качества политической коммуникации сегодня, конечно же, ранжируются и политически переосмысливаются правящими элитами и бюрократией в собственных интересах, однако они во многом определяются состоянием и уровнем развития общей и политической культуры данного общества. Политическая коммуникация, выступая способом, средством существования и передачи политической культуры, в свою очередь, сама опосредуется культурными нормами и ценностями.

**Примечания:**

[1] См.: *Cotteret J.-M.* Gouvernants et gouvernes: La communication politique. – P, 1973. – P.9, 112.
[2] *Ленин В.И.* Материализм и эмпириокритицизм // *Ленин В.И.* Полн. собр. соч. Т.18. С.348.
[3] *Винер Н.* Творец и робот. – М., 1966. С.41.
[4] См.: *Ланге О.* Целое и развитие в свете кибернетики // Исследования по общей теории систем. – М.,1969. С.183.
[5] м.: *Ланге О.* Целое и развитие в свете кибернетики // Исследования по общей теории систем. – М., 1969. С.184-185.
[6] *Винер Н.* Кибернетика и общество. – М., 1958. С.31.
[7] *Винер Н.* Кибернетика и общество. – М., 1958. С.30.
[8] *Винер Н.* Кибернетика, или управление и связь в животном и машине. – М.,1983. С.236.
[9] *Pye L.* Political Communication // The Blackwell Encyclopedia of Political Institutions. Oxford – New York, 1987. – P.442.
[10] *The Dictionary* of Political Analysis / Ed.: J.C.Plano, R.E.Riggs H.S.Robin. ABC – Clio. Canta Barbara. USA – Great Britain, 1982. P. 112.
[11] *Lasswell H.D.* The structure and function of communication in society // The Communication of Ideas. / Ed.: L. Bryson. – New York: Harper and Brothers, 1948. P.37.
[12] См.: *Braddock R.* An extension of the “Lasswell Formula” // *Journal of Communication*. – Vol. 8. – 1958. – P.88-93.
[13] См.: *Shannon K., Weaver W.* The Mathematical Theory of Communication. – Urbana: University of Illinois Press, 1949. P.5.
[14] *DeFleur M.* Theories of Mass Communication. – New York, 1970. P.90-91.
[15] *Cottret J.-M.* Gouvernants et gouvernes: La communication politique. – P, 1973. – P.7-13.
[16] См.: *Sinne K.* Communication: Mass Political Behavior // *Political Communication Issues and Strategies for Research*. – Vol.4. – L., 1975.
[17] *Маркс К., Энгельс Ф.* Манифест Коммунистической партии // *Маркс К., Энгельс Ф.* Сочинения. – 2-е изд. Т.4. – С.445.
[18] *Sanisteban L.S.* Fundaments de cencia politica. – Lima, 1986. P.76.
[19] См.: *Bordewijk J.L., Kaam B. van.* Allocute. – Baarn, 1982; *Bordewijk J.L., Kaam B. van.* Towards a classification of new teleinformation services // *Intermedia*. – 1986. – Vol. 14. – № 1. – P.16-21.
[20] *Bell D.* Die dritte tecnologische Revolution und ihre moglichen sociookonomischen Konsequenzen // *Mercur*. – Stuttgart, 1990. – Jg.44. – H.1. – S.34.
[21] *Винер Н.* Кибернетика и общество. – М., 1958. С. 30.
[22] См.: *Ito Y.* The “Johoka Sakai” approach to the study of communication in Japan // *Mass Communication Review*: Yearbook 2 / Eds: Wilhoit G.C., Bock H. – Beverly Hills, CA: Sage, 1981.
[23] См.: *Bell D.* The Social Framework of the Information Society. The Computer Age: A Twenty Year Wiew. – London, 1981; *Brzezinski Z.* The Grand Failure: The Birth and Death of Communism in the Twentieth Century. – New York, 1989; *Dahrendorf R.* Reflections of the the Revolution in Europe. – New York, 1990; *Masuda I.* The Information Society as Post-Industrial Society. – Washington, 1983; *Naisbitt J., Aburden P.* Megatrends 2000: The New Directions for the 1990’s. – New York, 1990; *Shaff A.* Perspektiven des modernen Sozialismus. – Wien; Zurich, 1987; *Кинг А., Шнайдер Б.* Первая глобальная революция: Доклад Римского клуба. – М., 1991; *Тоффлер О.* Третья волна. – М., 1992 и др.
[24] См.: *Martin W.J.* The Information Society. – London, 1988. P. 14-15.
[25] *Martin W.J.* The Information Society. – London, 1988. P. 42, 56.

[26] *Naisbitt J., Aburden P.* Megatrends 2000: The New Directions for the 1990's. – New York, 1990. P.302-303.
[27] См.: *Cuilenburg J.J. van.* The information society: some trends and implications // *European Journal of Communication*. – 1987. – Vol.2. – N 1. – P. 105-121.
[28] См.: *Моргунов Е.Б.* Человеческие факторы в компьютерных системах. – М., 1994. С. 18-19.
[29] См.: *McQuail D.* Media Performance. Mass Communication and the Public Interest. L. – N.P. – N.Delhi, 1993. – P.277.

**Источник:** Грачев М.Н. Политическая коммуникация // Вестник Российского университета дружбы народов. – Серия: Политология. – 1999.

*ЛЕБЕДЕВА М.М.*

# НОВЫЕ ТЕХНОЛОГИИ КАК ПОЛИТИКООБРАЗУЮЩИЙ ФАКТОР В МЕНЯЮЩЕЙСЯ СТРУКТУРЕ СОВРЕМЕННОГО МИРА

Технологический фактор всегда играл весьма значительную роль в политическом развитии общества, обеспечивая не только экономический и социальный прогресс, но и формируя во многом политическую систему мира. Об этом писал, в частности, еще А. Тоффлера, говоря о сельскохозяйственной, индустриальной и постиндустриальной эпохах[1]. Пожалуй, более четко на это указал Ф. Фукуяма в одной из последних своих статей, заметив, что индустриальная эпоха — эпоха паровоза, железных дорог, заводов сделала возможным веберовское централизованное государство[2]. Именно такое государство явилось своего рода «молекулой» построения политической системы, которая получила название «Вестфальской модели мира», поскольку ее формирование началось с подписания Вестфальского мира 1648 г. При этом, как замечает французский исследователь Ж.-М. Геено, создатели этой модели хорошо понимали, что формируемый ими миропорядок не мог строиться на ценностных ориентирах, в частности, на религии. Ценности не подлежат обсуждению и по ним не делают уступок. В результате в основу Вестфальской модели мира были положены национальные интересы, по которым возможен поиск компромиссных решений[3]. Стала выстраиваться система внутри- и межгосударственных отношений с присущей ей механизмами и аппаратом управления, путем которого вырабатывались и осуществлялись внутренняя и внешняя политика государств. Впоследствии эта модель получила еще одно название — государственно-центристской модели мира.

Вестфальская (или государственно-центристская) модель мира просуществовала до конца XX столетия, когда началась ее эрозия и на смену индустриальной эпохи пришла постиндустриальная, которая характеризуется использованием высоких технологий и биотехнологий, а на смену международной политике, по определению Дж. Розенау, пришла «постмеждународная политика», где наряду с государственными акторами стали активно действовать негосударственные участники[4]. Каковы же основные черты этой новой эпохи и какова роль новых технологий в политической трансформации мира?

## *1. Формирующаяся новая модель мира*

Существует множество концепций и подходов, в которых авторы пытаются осмыслить сущностные характеристики современной политической структуры мира, тенденции его развития. В одних концепциях мир становится все более гомогенным, главным образом, вследствие развития процессов глобализации, которые охватывают новые территории и затрагивают новые аспекты (экономические, социальные, культурные, политические и т.п.). В них глобализация обычно рассматривается как распространение западных моделей, ценностей, институтов и т.п. Классическими в этом плане являются работы Ф. Фукуямы[5].

В других теоретических схемах мир оказывается разделенным или расколотым. Причем, основания для раскола разные, в частности, ими выступают: западная,

---

[1] Toffler A. The Third Wave. — New York.: Morrow, 1980.

[2] Fukuyama F. Second Thoughts. The Last Man in a Bottle // The National Interest. — 1999. — Summer. — P. 26.

[3] Guehenno Jean-Marie. Globalization and International System // Journal of Democracy. — 1999. — N 7. — P. 22—35.

[4] См.: Rosenau J. Turbulence in World Politics. A theory of Change and Continuity. — Princeton: Princeton University Press, 1990.

[5] Fukuyama F. The End of the History? / The National Interest. — № 16 (Summer). — 1989. — P. 3—18; Fukuyama F. The End of the History and the Last Man. — N. Y.: The Free Press, 1992; Fukuyama F. Second Thoughts. The Last Man in a Bottle // The National Interest. — 1999. — Summer. — P. 16—33.

латиноамериканская, африканская, исламская, конфуцианская, хинди, православная, буддистская, японская цивилизации — у С. Хантингтона[6]; также цивилизации, но иного рода — сельскохозяйственная, индустриальная и постиндустриальная — у А. Тоффлера[7]; уровень профессионализма — у В.Л. Иноземцева[8]; уровень социально-экономического развития стран (высокий, средний и низкий, на основе чего, соответственно, выделяется центр, полупериферия, периферия) — у И. Валлерстейна[9], шесть пространственно-экономических зон (североатлантическая, тихоокеанская, евразийская, «южная», расположенная «преимущественно в районах индо-океанской дуги, а также два транснациональных пространства, выходящих за рамки привычной географической картографии») — у А.И. Неклесса[10]. В этих, а также в других аналогичных подходах, в которых подчеркивается дифференциация мира, особо указывается на реальные или потенциальные конфликты.

Наконец, существуют концепции, в которых делаются попытки совместить обе тенденции — глобализацию и универсализацию мира — с одной стороны, и его фрагментацию, обособление отдельных частей и областей — с другой. Одним из первых, кто попытался сделать это, был Б.Р. Барбер[11]. За ним последовали и другие. Так, директор СИПРИ А. Ротфельд пишет, что отношения в современном мире определяются, с одной стороны, центробежными процессами (глобализацией или интеграцией), а с другой — центростремительными (фрагментацией, эрозией государств)[12], а Дж. Розенау предложил даже специальный термин — «фрагмегративность» («fragmegrative» как одновременное действие фрагментации — «fragmentation» и интеграции — «integration»)[13], отражающий одновременно оба процесса — интеграцию и фрагментацию мира.

Независимо от того, какой именно точки зрения придерживаются исследователи, большинство из них подчеркивают, что в конце XX столетия мир переживает некий критический период, который определяется как «точка бифуркации»[14], «переходный возраст»[15], эпоха неопределенности, «переломности» и т.п. Это тот период, когда происходят качественные изменения, меняющие суть самой политической системы мира. Заметим, что подобных воззрений придерживаются не только сторонники неолиберальной традиции в международных исследованиях, которые особо подчеркивают этот момент, но и те, кто разделяет неореалистические взгляды. Так, Г. Киссинджер пишет, что мировой порядок и его составные части никогда еще не изменялись так быстро, глобально и глубоко[16].

В связи с кардинальными переменами в политической структуре мира в конце XX столетия все с большей настойчивостью стали говорить о кризисе, эрозии, закате Вестфальской модели мира[17], которая просуществовала более 350 лет, а вместе с ней и одного из центральных понятий в международных отношений — понятия «суверенитета». Надо сказать, что содержание понятия «суверенитет» не было незыблемым в истории. Оно

---

[6] Хантингтон С. Столкновение цивилизаций // Полис. — 1994. — № 1 — С. 33—48; Huntington S. The Clash of Civilizations and the Remaking of World Order. — New York.: Simon and Schuster, 1996.

[7] Toffler A. The Third Wave. — New York.: Morrow, 1980.

[8] Иноземцев В.Л. Расколатая цивилизация. — М.: «Academia» — «Наука», 1999.

[9] Wallerstein I. The Modern World-System. — N. Y.: Academic Press, 1974; Wallerstein I. The Politics of the World-Economy: The States, the Movements and the Civilizations. Cambridge: Cambridge University Press, 1984; Wallerstein I. The End of the World as We Know It: Social Science for the Twenty-First Century. — Minneapolis: University of Minnesota Press. — 2000.

[10] Неклесса А.И. Конец эпохи большого модерна. — М.: Институт экономических стратегий, 1999.

[11] Barber B.R. Jihad vs. McWorld // Atlantic Monthly. — March 1992. — P. 53—61.

[12] Rotfeld A. The Global Security System in Transition // Космополис. Альманах. — 1999. — С. 17—27.

[13] Rosenau J.N. New Dimention of Security: The Interaction of Globalizing and Localizing Dynamics // Security Dialogue, Vol. 25 (September 1994). — P. 255—282.

[14] Rosenau J.N Turbulence in World Politics. A Theory of Change and Continuity. — Princeton: Princeton University Press, 1990; Rosenau J.N. Along the Domestic-Foreign Frontier: Exploring Governance in a Turbulent World. — Cambridge: Cambridge University Press, 1997.

[15] Лебедева М.М., Мельвиль А.Ю. «Переходный возраст» современного мира // Международная жизнь. — 1999. — № 10. — С. 76—84.

[16] Kissinger Hentry. How to Achieve the New World Order // Time. — 1994. — March 14. — P. 73.

[17] См.: Космополис, 1999.

менялось и развивалось[18]. Тем не менее, в течение 350 лет ее «стержень» оставался прежним — и внутренняя политика, и внешняя были ориентированы на государственно-центристскую модель мира. Во внутренней политике именно государство обладало всеми властными полномочиями (отсюда и классические определения понятия «государства»), в системе же международных отношений государства являлись фактически единственными структурными «единицами» взаимодействия.

Именно эта государственно-центристская модель стала разрушаться во второй половине XX столетия, сначала — лишь как тенденция, когда на политическую арену стали все активнее выходить межправительственные организации — ООН, а затем и создаваемые в различных сферах (например, в торговле ГАТТ), а также в регионах (например, в Европе НАТО, ОВД, ОБСЕ и т.д.) региональные организации. При их создании предполагалось, что они явятся своеобразными «проводниками» политики государств-создателей. Однако постепенно становилось очевидным, что эти организации все больше и больше стали играть вполне самостоятельную роль и уже сами оказывают значительное влияние как на международные отношения в целом, так и на своих создателей. Произошел сложный процесс взаимодействия и взаимовлияния государственных структур и международных организаций.

Конец XX столетия внес еще более серьезные коррективы в политическое развитие мира, когда на мировой арене в качестве политических участников активно стали выступать не только межправительственные организации, но и неправительственные, такие как транснациональные корпорации, СМИ, экологические (например, «Greanpeace»), профессиональные (например, «Врачи без границ»), феминистские и т.п.

Одновременно самостоятельно стали действовать внутриполитические регионы. Так, например, Шотландия заявляла о своем стремлении войти в структуры ЕС на правах полноправного члена. Внутригосударственные регионы становятся значимым фактором европейского строительства, что привело даже к появлению такого понятия, как «Европа регионов»[19]. Иными словами, даже в одном регионе наряду с процессами интеграции четко прослеживаются процессы обособления и самостоятельной деятельности отдельных элементов общей интегративной структуры.

Конечно, существуют и возражения (в основном высказываемые в рамках неореалистических представлений), согласно которым Вестфальская система мира сохраняется, т.к. сохраняются государственные границы в мире, количество государств становится не меньше, а, напротив, больше, увеличиваются возможности государств воздействовать на своих граждан, государства сами активно создают международные институты и режимы[20], наконец, вообще неясно, чем могут быть они заменены государства. И все же, если под суверенитетом понимать то, что американский исследователь С.Д. Краснер назвал «Вестфальским суверенитетом», т.е. такую политическую организацию, которая основана на том, что внешние акторы фактически не могут воздействовать на внутреннюю политику или могут, но крайне ограничено[21], то такой суверенитет действительно стал размываться, а вместе с ним и государственно-центристская модель мира. Многие исследователи видят в процессе все большей транспарентности государственных границ суть глобализации[22].

### *2. Вклад новых технологий в формирование политической структуры мира*

---

[18] Сергеев В.М. Государственный суверенитет и эволюция системы международных отношений // Космополис. Альманах. — 1999. — С. 27—31.

[19] Иванов И.Д. Европа регионов. М.: Международные отношения. 1998.

[20] Подробнее эти аргументы и их критику см.: Фергюсон Й. Глобальное общество в конце двадцатого столетия // Международные отношения социологические подходы / Под ред. проф. П.А. Цыганкова. М. Гардарика, 1998. — С. 195—221.

[21] Krasner St. D. Sovereignty: Organized Hypocrisy. — Princeton: Princeton University Press, 1999.

[22] Katzenstein P.J., Keohane R.J., Krasner St. D. International Organization and the Study of World Politics // International Organization. — 1998. — V. 52. — N 4. — P. 645—686; Kegley Ch. and Wittkopf W. World Politics: Trend and Transformation. Seventh Edition. — New York: St. Martin's / WORTH, 1999.

Одним из ведущих факторов эрозии Вестфальской модели и формирования новой политической структуры мира стали новые технологии. Именно новые технологии делают межгосударственные границы наиболее прозрачными. Об этом довольно много публикаций на Западе и практически отсутствуют дискуссии в отечественной литературе. Роль новых технологий в современном мире крайне сложна и неоднозначна, видимо, именно по этой причине она не в полной мере оценена.

Прежде всего, необходимо определить, что следует понимать под новыми технологиями (НТ). Ф. Фукуяма пишет о двух революциях, идущих в настоящее время параллельно. Первая — в области высоких технологий (ВТ), включающей в себя, прежде всего, информационные (ИТ) и коммуникационные технологии (КТ), вторая — в области биотехнологий (БТ). Изменения, которые порождают информационные технологии и их вклад в формирование новой структуры мира более очевидны. Роль биотехнической революции, как полагает Ф. Фукуяма, более фундаментальна. Тем не менее, обе они взаимодействуют и непосредственно влияют на формирующуюся политическую структуру постиндустриального мира.

Заметим, что развитие новых технологий не только формирует новый мир, но и меняет наши образы о нем. Если мир Вестфальской системы национальных государств описывался образами и метафорами, взятыми из механики, физики и химии прошлых веков, где ядро и периферия были главными структурными элементами, то для формирующейся структуры мира ищутся образы уже из сферы новых технологий — мир выступает скорее как сложная паутина сети по типу Интернета. Именно такую метафору использует, например, Дж. Розенау[23].

Революция в области высоких технологий может быть рассмотрена как взаимосвязь между тремя компонентами[24]: 1) порождение новых знаний (за счет возможностей, которые открывают банки данных, Интернет и т.п.); 2) передача знаний — большие массивы информации передаются большому количеству людей; 3) появление новых материальных носителей, способствующих развитию, как ускоренной передачи информации и больших массивов, так и созданию и хранению информационных массивов (например, на основе квантовых компьютеров[25]).

Новые информационные и коммуникативные технологии, особенно повлияли на целый ряд аспектов политической жизни[26]. В результате чего меняется традиционная для эпохи господства Вестфальской модели мира постановка проблем безопасности, дипломатии, суверенитета и т.д. В образной форме это сформулировал обозреватель «Нью-Йорк Таймс» Томас Фридман в нашумевшей книге «Лексус и оливковое дерево», весьма образно заметив, что если символами «холодной войны были стена, разъединяющая миры, а также «горячая линяя» между Москвой и Вашингтоном, позволявшая, по крайней мере, сверхдержавам до определенной степени контролировать развитие этого «разъединенного» мира, то символом современной эпохи стал Интернет, при помощи которого все участники мирового сообщества «управляют» миром и вместе с тем никто не имеет всеобщего контроля над ним. В эпоху «холодной войны» традиционный вопрос о могуществе сводился к тому, сколько и какими боеголовками располагаете вы и ваш противник?». Сегодня этот же вопрос

---

[23] Rosenau J.N. Material and Imagined Community in Globalized Space / Globalization and Regional Communities: Geoeconomic, Sociocultural and Security Implications for Australia. — Toowomba (Australia): USQ Press, 1997. — P. 24—40.

[24] Snow, Donald M. The Shape of the Future: The Post-Cold War World. — N. Y.: M. E. Sharpe, 2nd ed., 1995. — P. 65—71.

[25] Подробнее см.: Медовников Д., Тюменев В. Считающий атом // Эксперт. — 2000. — № 17 (8 мая). — С. 25—27.

[26] См. Ferguson Y.H., Mansbach R.W. Technology and the Transformation of Global Politics // Paper prepared for the 2000 annual meeting of International Studies Association. — Los Angeles, March, 2000; Knowledge and Diplomacy // Ed. by Jovan Kurbalija. — Malta: DiploProjects Mediterranean Academy of Diplomatic Stusiea University of Malta, 1999; Snow Donald M., Brown Eugene. International Relations: The Changing Contours of Power. — New York a. o.: Longman, 2000.

звучит по-другому: «Насколько быстро работает ваш модем?»[27]. В результате, например, на рубеже веков зависимость в космосе становится в большей степени экономическим фактором, чем военным[28].

Информация, благодаря новым технологиям, значительно легче, чем товары, способна проникать через границы. Доступ к информации, а также скорость ее получения изменили глобальные и региональные структуры. Это имеет целый ряд следствий. С одной стороны, проникновение информации сквозь границы способствует глобализации и демократизации мира, ограничению возможности авторитарного управления и изоляционизма[29], ускорению темпов экономического развития. Все труднее становится «оградить» свою страну от информации «извне», хотя в некоторых государствах это и пытаются делать, ограничивая доступ в Интернет за счет контроля над провайдерами. Тем не менее, такая политика становится все дороже[30].

Использование (или неиспользование) новых технологий значительно влияет на статус страны: оказывается ли она интегрированной в мировое сообщество или, напротив, — в изоляции. Здесь следует иметь в виду, что некоторые страны особое внимание уделяют использованию новых технологий, хотя при этом могут отставать по ряду других экономических и социальных параметров. Так, в Южной Африке изначально широкое распространение получила система банкоматов, а также сотовых телефонных сетей. Однако уровень жизни африканского населения оставался крайне низким. С другой стороны, государства крайне различаются по тому, какие именно новые технологии они разрабатывают. Так, в Болгарии больше пользователей Интернет, чем во всей Африке к югу от Сахары, включая ЮАР[31].

Еще одним положительным моментом развития высоких технологий является улучшение коммуникаций между государствами в условиях кризиса. Вообще недостаток информации, ее искажение является одним из ключевых моментов развития кризисных отношений. В этом плане показателен опыт Карибского кризиса и решение об установлении «горячей линии» между Москвой и Вашингтоном.

Одновременно новые технологии все менее значимой делают национальную территорию. Через сеть Интернет человек оказывается вовлеченным в различные «клубы по интересам», выходящими далеко за пределы национальных границ. Более того, создаются даже виртуальные «государства». Об одном таком «государстве» — «Свободная Бирманская Коалиция» (Free Burma Coalition) — упоминают Й. Фергюсон и Р. Мэнсбач[32]. Это государство территориально находится лишь в киберпространстве и «предлагает свою солидарность, которая трудно достижимо географически»[33]. Все это фактически создает новую «профессиональную» или «корпоративную» идентичность и делает различные виды «столкновений» по территориальному принципу менее вероятными.

Вообще территории в современную эпоху «формируются» по иным принципам, далеко не всегда совпадающим с национальными границами — по принципам, в значительной степени ориентированным на информационные и интеллектуальные ресурсы, по типу Силиконовой долины. Так, довольно показателен в этом отношении электромагнитный спектр коммуникационных линий Земли, сделанный из космоса. Эти

---

[27] Friedman Th. L. The Lexus and the Olive Tree: Understanding Globalization. — N. Y.: Farrar Straus Giroux, 1999.

[28] Strategic Assessment 1999. Prioreties for a Turbulent World. Wash. (D. C.): National Defense University, Institute for National Strategic Studies, 1999. — P. 304.

[29] Ferguson Yale H., Mansbach Richard W. Technology and the Transformation of Global Politics // Paper prepared for the 2000 annual meeting of International Studies Association. — Los Angeles, March, 2000.

[30] Nye J.S. Responses to Fukuyama // The National Interest. — 1999. — Summer. — P. 43—44.

[31] UNDP, Human Development Office, Human Development Report, 1999. — New York: UNDP, 1999. — P. 62.

[32] Ferguson Yale H., Mansbach Richard W. Technology and the Transformation of Global Politics // Paper prepared for the 2000 annual meeting of International Studies Association. — Los Angeles, March, 2000.

[33] Arachnophilia // The Economist, August 10 — 16, 1996. — P. 28.

линии покрывают, главным образом, Европу, Северную Америку, Средиземноморское побережье Африки, Юго-Восточную Азию[34].

Формирование новых интеллектуальных центров имеет и оборотную сторону. Во-первых, все жестче для многих стран встает проблема «утечки мозгов». Во-вторых, государственные структуры все в большей степени теряют властные полномочия. Государству сложнее становится контролировать национальную экономику, особенно ее финансовую систему (как наиболее мобильную часть, о чем, например, свидетельствуют финансовые кризисы 1997—1998 годов в Юго-Восточной Азии и России), предпринимать те или иные секретные действия[35].

В-третьих, происходит расслоение населения Земного шара на тех, кто владеет новыми технологиями, и тех, кто ими не владеет и в результате во многом оказывается вне процессов глобализации и становится все ощутимее.

В-четвертых, прозрачными становятся не только территориальные границы, но и информация, ее доступность. Это, в свою очередь, порождает еще одну проблему — проблему информационного терроризма. Данный факт довольно хорошо осознается как серьезная угроза, причем, не только национальной безопасности, но и безопасности в широком смысле этого слова. Не случайно, в мае 2000 г. в Париже состоялась встреча участников «большой восьмерки» по компьютерному терроризму. Она включила в себя юристов, экспертов в области высоких технологий, государственных чиновников, представителей ведущих частных корпораций. Кибертерроризм, как подчеркивали участники, представляет собой серьезнейшую угрозу для человечества, сравнимую с ядерной, химической, бактериологической войной. США, которые добились наибольшего успеха в борьбе с терроризмом, выступают за создание кибернетической полиции с самыми широкими полномочиями. И здесь возникают противоречия. Европейцы, остерегаясь монополии и диктата со стороны США (и политической и экономической), вновь обращаются к проблеме национального суверенитета. При этом Франция предлагает взять за основу сотрудничества проект, разработанный в рамках Совета Европы, и не допустить компьютерных центров с наиболее благоприятными условиями, как это было в области финансов. Премьер-министр же Франции Лионель Жоспен в обращении к участникам довольно жестко заявил: «Свобода ценнее всех благ, которые дает нам Интернет»[36].

Если применение высоких технологий, несмотря на все противоречия, которые они порождают, все же в целом являются одним из наиболее существенных факторов глобализации (со всеми ее противоречиями и проблемами[37]), то этого нельзя сказать об использовании биотехнологий. Вообще, о биотехнологиях как политикообразующем факторе современности пишется значительно меньше. В основном литература посвящена вопросам, связанным, например, с решением проблем голода или медицинских проблем (замена органов). Более глобальные аспекты затрагиваются реже. В этом отношении статья Ф. Фукуямы «Переосмысливая: последний», опубликованная в 1999 г.[38], является скорее исключением. Он отмечает, что именно от биотехнологий следует ожидать наиболее радикальные изменения, а именно: изменения самого человека, в частности, путем контроля агрессивного поведения.

Проблема контроля поведения — не новая проблема, на что указывает и сам Ф. Фукуяма, говоря, что она ставилась, в частности, в фашистской Германии. Вопрос заключается в том, насколько следует регламентировать национальные программы в этой области. Ответ Ф. Фукуямы

---

[34] Strategic Assessment 1999. Prioreties for a Turbulent World. Wash. (D. C.): National Defense University, Institute for National Strategic Studies, 1999. — P. 313.

[35] Snow Donald M., Brown Eugene. International Relations: The Changing Contours of Power. — New York a. o.: Longman, 2000.

[36] Новые Известия, 17 мая 2000 г. — С. 3.

[37] Подробнее см.: Лебедева М.М., Мельвиль А.Ю. «Переходный возраст» современного мира // Международная жизнь. — 1999. — № 10. — С. 76—84.

[38] Fukuyama F. Second Thoughts. The Last Man in a Bottle // The National Interest. — 1999. — Summer. — P. 16—33.

состоит в том, что делать это не следует, поскольку, с одной стороны, это невозможно, с другой — подобные регламентации повлекут за собой регламентации и в другой области — в области информационных технологий. Представляется, что подобная политика может привести как раз к тому, против чего выступает Ф. Фукуяма — автономизации и «де-демократизации», поскольку открывают авторитарным режимам довольно широкие возможности управления поведением.

Вместе с тем, Ф. Фукуяма замечает, что переход от индустриального к постиндустриальному миру представляет собой совершенно иные экономические условия, где производство открывает дорогу к обслуживанию, где резко возрастает образовательный уровень, где интеллект заменяет материальное производство, и где технологии и технологические инновации становятся все проникающими, а сложность экономических отношений возрастает по экспоненте. Это требует регуляции этой сложности. Видимо, именно в том, какая должна быть регуляция и, какова роль государства в создании регуляционных механизмов лежит ответ на вопрос о контроле за использованием новых технологий.

Вообще о роли государства в формирующемся новом мире существуют различные точки зрения. Так, Дж. Розенау склонен полагать, что государства все более теряют объем своих властных полномочий[39], и выполняют свою лидирующую роль на мировой арене в значительной мере по инерции[40]. С ослаблением роли государства на мировой арене нередко связывается и кризис межгосударственных организаций (прежде всего, ООН), их излишняя бюрократизация, неспособность быстро и адекватно реагировать на новые вызовы и даже взаимодействие с неправительственными и межправительственными организациями[41]. Если рассматривать роль государства в крайне далекой исторической перспективе, то с такой оценкой можно было бы согласиться. Однако необходимо признать и другое. Государства на сегодняшний день, будучи ведущими акторами на мировой арене, могут оказывать и реально оказывают наиболее сильное воздействие на мир и формирующуюся новую систему взаимоотношений. Представить, что государства окажутся пассивными в этом процессе и добровольно «уйдут» с мировой арены, добровольно сдав свои властные полномочия неизвестно кому, просто невозможно.

В принципе процесс рождения новой структуры мира, создание его новой архитектуры реально может идти следующими путями. Один путь – хаотичный, плохо управляемый, с «перетягиванием каната» между различными государствами, а также другими участниками международных отношений, применением силы и т.п. Этот путь скорее ведет к реализации прогнозов тех исследователей, которые полагают, что в лучшем случае новый XXI век будет больше похож на пестрое и беспокойное средневековье, в худшем – нам грозит вселенская катастрофа[42].

Второй путь – путь кризисного управления, путь активного поведения государства (кстати, о таком понимании сильного государства упоминал и Генеральный секретарь ООН Кофи Аннан в Нью-Йорке 3 апреля 2000) предполагает и «выстраивание» новых структур и формирование нового мироустройства с учетом новых реалий и интересов различных участников-государств, межгосударственных организаций, неправительственных объединений, крупнейших финансовых и бизнес структур. При этом государство может оказывать наиболее сильное воздействие на мир и в этом смысле, используя метафору из области ядерной физики, не допустить «неуправляемого распада» Вестфальской системы

---

[39] См.: Governance Without Government: Order and Change in World Politics // Ed. by J.N. Rosenau, E.-O. Szempiel. — Cambridge: Cambridge University Press, 1992.

[40] Rosenau J.N. Material and Imagined Community in Globalized Space / Globalization and Regional Communities: Geoeconomic, Sociocultural and Security Implications for Australia. — Toowomba (Australia): USQ Press, 1997. — P. 24—40.

[41] Фергюсон Й. Глобальное общество в конце двадцатого столетия // Международные отношения социологические подходы / Под ред. проф. П.А.. Цыганкова. М. Гардарика, 1998. — С. 195—221.

[42] Бус К. Вызовы незнанию: Теория международных отношений перед лицом будущего / Международные отношений социологические подходы // Под ред. П.А. Цыганкова. — М.: Гардарика, 1998. — С. 307—331.

мира.

На этом пути, правда, существуют свои «подводные камни», на которую в последнее время все больше обращают внимание. Речь идет о возможности нелегальных видов бизнеса использовать официальные, в том числе и дипломатические каналы, для построения иного мироустройства, с законами и правилами поведения по принципу «диких джунглей»[43]. В настоящее время в этом плане обсуждается в основном наркобизнес. Однако не меньшая, если не большая опасность, исходит от возможности сращивания криминальных структур с государственными в некоторых странах и использования ими новых технологий для получения максимального объема властных полномочий.

Попытка выбрать еще один путь — путь ориентации на «отстранения» от внешнего мира, сосредоточение на внутренних проблемах для того, чтобы, затем уже с иным экономическим и политическим потенциалом, вновь вступить в международные отношения, неоправданна по ряду причин. Во-первых, это практически невозможно сделать в силу сильной экономической, технологической и т.п. взаимозависимости мира. Во-вторых, темпы современного развития, прежде всего благодаря новым технологиям, в настоящее время настолько велики, что любая изоляция или самоизоляция неизбежно приведут к тому, что государство, избравшее этот путь, окажется в стороне от исторического процесса.

Очевидно, что на практике не существует ни одного из названных путей «в чистом виде». Элементы каждого из них, так или иначе, проявляются. Вопрос заключается в том, какой в целом вектор развития окажется доминирующим.

**Источник:** Лебедева М.М. Новые технологии *как* политикообразующий фактор *в* меняющейся структуре современного мира // Мир и Россия на пороге XXI века: Вторые Горчаковские чтения. Антология. М.: Российская политическая энциклопедия, 2001. С. 94 – 105.

[43] См., напр., Nyerere J. Peace Comes From Justice, Not Absence Violence // Peace Initiatives. — 1997. — V. III. — N2 (March—April).

*БЕЛЛ Д.*

# СОЦИАЛЬНЫЕ РАМКИ ИНФОРМАЦИОННОГО ОБЩЕСТВА

*Об авторе*. Дэниел Белл (Bell, Daniel) (р. 1919), американский социолог и публицист, член Американской академии искусств и наук. Родился 10 мая 1919 в Нью-Йорке. По окончании учебы преподавал социологию в Колумбийском (1959-1969), а затем в Гарвардском университете (с 1969 по настоящее время). Первая же крупная публикация Белла - книга Конец идеологии (The End of Ideology, 1960) - создала ему репутацию одного из ведущих американских теоретиков в области социальных и политических наук. Наряду с Артуром Шлезингером-младшим Белл возглавил т.н. "школу консенсуса" - либерально-центристское течение, доминировавшее в интеллектуальной жизни Америки 1950-х годов. Ключевым тезисом этой школы стало утверждение об исчерпанности традиционных политических идеологий. Коммунизму, фашизму и другим "программным" идеологиям Белл противопоставил либеральную приверженность умеренному социальному реформизму, свободному рынку и индивидуальным гражданским свободам. В отличие от либеральных теоретиков националистического склада (таких как Дэниел Бурстейн) или неоконсерваторов (таких как Ирвинг Кристол), Белл не стремился преувеличивать степень культурной однородности американского общества или распространенности ценностей среднего класса.

*Вечная гонка по кругу идей и новаций,*
*Изобретений, открытий, экспериментов*
*Откроет нам сущность движения, но не покоя.*
*О жизнь, растраченная в существовании...*
*О мудрость, утраченная в знании...*
*О знание, потерянное в информации...*
***Т. С. Элиот***

**Информация и телекоммуникации в постиндустриальном обществе**

В настоящем столетии решающее значение для экономической и социальной жизни, для способов производства знания, а также для характера трудовой деятельности человека приобретет становление нового социального уклада, зиждущегося на телекоммуникациях. Революция в организации и обработке информации и знаний, в которой центральную роль играет компьютер, развертывается одновременно со становлением постиндустриального общества. Три аспекта постиндустриального общества особенно важны для понимания телекоммуникационной революции:

- переход от постиндустриального общества к сервисному обществу;
- решающее значение кодифицированного теоретического знания для осуществления технологических инноваций;
- превращение новой "интеллектуальной технологии" в ключевой инструмент системного анализа и теории принятия решений.

Показатели перехода от постиндустриального к сервисному сектору достаточно очевидны. В США в 1970 г. 65% рабочей силы было занято в сфере услуг, около 30 - в промышленности и строительстве и неполных 5% - в сельском хозяйстве. Однако осевым принципом постиндустриального общества является громадное социальное значение теоретического знания и его новая роль в качестве направляющей силы социального изменения. Каждое общество функционировало на основе знания, но только во второй половине XX века произошло слияние науки и инженерии, изменившее самую сущность технологии. Промышленные отрасли, пока что доминирующие в обществе, - сталелитейная, моторостроение, электротехническая, телефонная, авиастроительная - представляют собой "промышленность XIX века" (хотя литье стали было освоено в XVII веке, а авиация - в XX веке) в том отношении, что все они были созданы "талантливыми жестянщиками", которые

работали независимо от какой бы то ни было науки и в полном ее неведении. Александр Белл - изобретатель телефона - был преподавателем ораторского искусства, принцип телефона он открыл в поисках средства, которое помогало бы лучше слышать людям с плохим слухом. Бессемер, разработавший доменный процесс для усовершенствования литья пушек, не знал научных работ Генри Сорби по металлургическим процессам. А Томас Альва Эдисон, по-видимому, наиболее изобретательный и талантливый из этих "жестянщиков" (среди прочего он изобрел электрическую лампу, фонограф, "движущиеся картинки"), был совершенно несведущ в математике и не имел ни малейшего представления о теоретических уравнениях Кларка-Максвелла по электромагнитным свойствам вещества.

Изобретательство в XIX веке было сугубо эмпирическим процессом проб и ошибок, время от времени озаряемых блистательными прозрениями. Сущность же современной развитой технологии - в ее органически тесных отношениях с наукой; здесь исследователь заинтересован не столько в конечном продукте своей работы, сколько в познании разнообразных свойств материалов и основных принципов их комбинаций, сочетаний и замещений. Как отмечает выдающийся металлург С. Смит, в наше время "материалы стали рассматриваться в сравнении, с точки зрения их свойств, необходимых для того или иного применения. Каждая новая технологическая разработка - радар, ядерный реактор, реактивный двигатель, компьютер, спутник связи - по-своему разрушала прежнюю модель, в которой каждый данный материал был связан с каждым данным видом продукта. Так возникла современная инженерия".

Сущность этого изменения, как в технологии, так и в науке, связана с расширением "поля отношений" теории и сферы ее применения, вследствие чего становится возможной систематическая синергия в открытиях и разработках новых продуктов и теорий. Наука в своих основаниях - это набор аксиом, топологически связанных в унифицированную схему. Но, как заметил Броновский, "новая теория изменяет систему аксиом и устанавливает новые связи на стыках, что изменяет топологию. Когда две науки объединяются в одну, новая сеть оказывается более богатой и четкой, чем простая сумма двух частей".

По мере того, как современная наука, как впрочем, и почти все остальные виды человеческой деятельности, движется по пути все большей специализации, дабы детализировать свои концепции, наиболее важным результатом ее связей с технологией становится интеграция различных областей или наблюдений в единую теоретическую систему, имеющую все большую продуктивность.

Основным методологическим достижением второй половины XX века стало управление организованными множествами - теориями множеств с большим числом переменных и комплексными организациями и системами, требующими координации деятельности сотен тысяч и даже миллионов людей. Начиная с 40-х годов, шло бурное развитие новых областей научного знания, связанных именно с этими проблемами организованных множеств: информационной теории, кибернетики, теории принятия решений, теории игр, теории стохастических процессов. В этих дисциплинах был разработан ряд специальных методик, таких, как линейное программирование, статистическая теория решений, цепи Маркова, метод Монте-Карло, метод экстремальных стратегий, которые позволяют выявлять определенные закономерности из больших множеств, получать оптимальные решения из различных альтернатив или, во всяком случае, определять рациональные моменты в условиях неопределенности.

Поскольку технология есть инструментальный способ рационального действия, я назвал эти новые разработки "интеллектуальной технологией", так как все они дают возможность поставить на место интуитивных суждений алгоритмы, то есть четкие правила принятия решений. Эти алгоритмы могут быть материализованы в автоматической машине, выражены в компьютерной программе или наборе инструкций, основанных на какой-либо статистической или математической формуле, представляющей собой способ формализации суждений и их стандартного применения во многих различных ситуациях. Поскольку интеллектуальная технология становится основным инструментом управления

организациями и предприятиями, можно сказать, что она приобретает столь же важное значение для постиндустриального общества, какое для общества индустриального имела машинная технология.

**Информационная теория стоимости**

Когда знание в своей систематической форме вовлекается в практическую переработку (в виде изобретения или организационного усовершенствования), можно сказать, что именно знание, а не труд выступает источником стоимости. Экономисты в своих концепциях, объясняющих производство и обмен, используют в качестве основных переменных "землю, капитал и труд". Более проницательные исследователи, - например, В. Зомбарт и Й. Шумпетер - дополняют эту триаду такими важными понятиями, как "деловая инициатива" и "предприимчивость". Но, несмотря на это, доминирует все же такой аналитический подход к экономике, который акцентирует те или иные комбинации капитала и труда в духе трудовой теории стоимости, почти полностью игнорируя при этом роль знания или организационных новшеств и управления. Однако с сокращением рабочего времени и с уменьшением роли производственного рабочего становится ясно, что знания и способы их практического применения замещают труд в качестве источника прибавочной стоимости. В этом смысле, как труд и капитал были центральными переменными в индустриальном обществе, так информация и знания становятся решающими переменными постиндустриального общества.

**Использование моделей**

Хотя технологические революции идеальны в своих теоретических основаниях, их символами, чтобы не сказать носителями, являются все же некие материально-вещные формы, и в постиндустриальном обществе эта "вещь" - компьютер. Если, как сказал П. Валери, электричество было агентом трансформации общества второй половины XIX века, то компьютер - в качестве "аналитической машины" точно так же трансформирует общество второй половины XX века. Электричество как источник света, энергии и коммуникации вызвало к жизни "массовое общество", т.е. в громадной степени расширило социальные связи и взаимодействия между людьми и тем самым многократно усилило то, что Э. Дюркгейм называл социальной плотностью общества. В этой связи можно сказать, что компьютер является инструментом управления массовым обществом, поскольку он есть механизм обработки социальной информации, громадный объем которой растет почти экспоненциально в силу расширения социальных связей.

Основная социально-политическая проблема массового общества - можем ли мы управлять экономикой достаточно эффективно, чтобы достичь наших общественных целей. Появление компьютеров позволило нам создавать детализированные модели экономики. Ясно, что экономисты вполне научились моделировать экономику и осуществлять компьютерный анализ альтернативных политик, дабы лучше уяснить себе их возможные последствия, - гораздо менее ясно, однако, могут ли такие модели помочь нам управлять экономикой. Дело в том, что для любого общества главные решения - политические, а эти решения не являются производными от экономических факторов.

Можно ли смоделировать общество? Здесь сразу же возникает та проблема, что у нас отсутствует сколько-нибудь убедительная теория о том, каковы силы внутреннего сцепления социального механизма, хотя, как это ни парадоксально, благодаря нашему пониманию технологии мы лучше представляем себе, как общество изменяется. Моделировать можно лишь закрытую или конечную систему. Однако общество становится все более открытым и индетерминированным, и, по мере того как люди все яснее осознают свои цели, дебаты относительно решений обостряются. Решения по проблемам социальной политики становятся все в большей степени делом политической сферы, а в меньшей - совокупного рынка, а это опять-таки ведет к уменьшению наших возможностей моделировать общество.

**Слияние технологий**

В XIX и вплоть до середины XX века коммуникации существовали в двух различных формах. Первая - это почта, газеты, журналы и книги, т.е. средства, которые печатались на

бумаге и распространялись методом физической транспортации или хранились в библиотеках. Вторая - это телеграф, телефон, радио и телевидение; здесь закодированные сообщения или речь передавались средствами радиосигналов или по кабельной связи от человека к человеку. Сейчас технологии, некогда существовавшие в разных областях применения, стирают эти различия, так что потребители информации получают в свое распоряжение множество альтернативных средств, что порождает и ряд сложных проблем с точки зрения законодательства.

В дело с неизбежностью вовлекаются мощные частные интересы. Точно так же как замена угля нефтью и конкуренция между грузовым автотранспортом, железными дорогами и газопроводами привели к существенным изменениям в распределении корпоративной власти, в структурах занятости, в профсоюзах, географическом расположении предприятий и тому подобном, так и колоссальные изменения, происходящие в коммуникационной технологии, затрагивают отрасли промышленности, связанные с коммуникациями.

В самом общем плане здесь можно выделить пять основных проблем. Слияние телефонных и компьютерных систем, телекоммуникаций и обработки информации в одну модель. С этим связан вопрос, будет ли передача информации осуществляться преимущественно через телефонную связь или возникнет какая-либо иная независимая система передачи данных; какова будет относительная доля микроволновых станций, спутников связи и коаксиального кабеля в качестве каналов передачи.

Замена бумаги электронными средствами, включая электронные банковские услуги вместо использования чеков, электронную почту, передачу газетной и журнальной информации факсимильными средствами и дистанционное копирование документов. Расширение телевизионной службы через кабельные системы со множеством каналов и специализированными услугами, что позволит осуществлять прямую связь с домашними терминалами потребителей. Транспорт будет заменен телекоммуникациями с использованием видеофонов и систем внутреннего телевидения. Реорганизация хранения информации и систем ее запроса на базе компьютеров в интерактивную информационную сеть, доступную для исследовательских групп; прямое получение информации из банков данных через библиотечные и домашние терминалы. Расширение системы образования на базе компьютерного обучения, использование спутниковой связи для сельских местностей, особенно в слаборазвитых странах; использование видеодисков, как для развлечений, так и для домашнего образования. Технологически телекоммуникации и обработка информации сливаются в единую модель, получившую название "компьюникация". По мере того как компьютеры все шире используются в коммуникационных сетях в качестве коммутирующих систем, а средства электронной коммуникации становятся неотъемлемыми элементами в компьютерной обработке данных, различия между обработкой информации и коммуникацией исчезают. Основные проблемы здесь - правовые и экономические, и основной вопрос - должна ли эта новая область подлежать государственному регулированию или ей лучше развиваться в условиях свободной конкуренции.

Самый же важный аспект - политический. Информация - это власть. Доступ к информации есть условие свободы. Из этого прямо вытекают проблемы законодательного характера. Такие электронные средства информации, как телевидение, регулируются юридическими нормами "честности" и права дать ответ. Телефонная индустрия также регулируется в том, что касается тарифов и условий предоставления услуг. Компьютерная отрасль пока не подлежит государственному регулированию и развивается в условиях свободного рынка. Не регулируются и печатные средства информации; их права на свободу слова гарантированы Первой поправкой к конституции и охраняются судами. Библиотеки преимущественно контролируются частными лицами или местной властью. Сейчас правительственные агентства и частные корпорации создают гигантские банки данных. Должны ли эти банки данных быть под правительственным наблюдением или им лучше развиваться без правительственного контроля? Это важнейший для будущего свободного общества вопрос.

**Политика в информационном обществе**

Я исхожу из того, что знания и информация становятся стратегическими ресурсами и агентом трансформации постиндустриального общества. Бурное протекание общественных изменений, особенно когда они, как в данном случае, осуществляются через посредство специфических технологий, с неизбежностью ставит перед обществом сложные политические проблемы. Здесь можно лишь схематически обозначить некоторые из проблем, которые общество будет вынуждено решать в ближайшие два десятилетия.

Новая инфраструктура. Каждое общество внутренне связано различными каналами, позволяющими его членам осуществлять материальный и духовный обмен. Организация, финансирование, поддержание и управление этими каналами, или инфраструктурой, обычно находились в компетенции правительства. Первой инфраструктурой был транспорт - дороги, каналы, железнодорожные и воздушные магистрали; все это позволяло связывать воедино различные локалитеты общества и осуществлять перемещение товаров и людей. Второй инфраструктурой были средства передачи энергии - водяное колесо, паровые машины, газ, электричество, нефтепроводы. Мобилизуя не столько природные, сколько технологические источники энергии и связывая их в единые энергетические сети, человечество не только радикально изменило городскую жизнь, но и обеспечило себя энергией для производства товаров в массовом масштабе и применения разнообразной бытовой техники. Третьей инфраструктурой были коммуникации - вначале почта и газеты, затем телеграф и телефон, сейчас радио и телевидение; все это сыграло роль каналов колоссального информационного взрыва, своего рода бомбардировки сенсорного аппарата человека, расширения социального и психологического взаимодействия людей, которое сейчас растет экспоненциально.

В предстоящие два десятилетия какие-либо изменения в первой инфраструктуре - на транспорте - маловероятны. Даже если освоение "Конкорда" или какого-либо другого сверхзвукового самолета вдвое сократит время перелета через океан, это отнюдь не возымеет того значения, которое имели последовательные этапы сокращения времени, необходимого для пересечения Атлантики, в течение последних ста лет - с нескольких недель плавания первыми пароходами, до шести дней - пароходами более мощными, затем до 16 часов - турбовинтовыми самолетами и, наконец, до 7 часов самолетами реактивными. Даже если в прежних масштабах возродится общественный транспорт, маловероятно, чтобы он вытеснил личный автомобиль, если только рост цен на бензин в будущем не разрушит гедонистический образ жизни, столь глубоко укоренившийся в развитых индустриальных обществах.

Во второй инфраструктуре - энергетической - есть некоторые новые тенденции. Они, однако, требуют больших капиталовложений в такие области, как консервация энергии, усовершенствование техники добычи угля и его газификации, использование ядерной энергетики, более эффективная передача электричества по проводникам, освоение солнечной энергии. Эти проблемы могут стимулировать колоссальное расширение исследований и разработок и в случае успеха - создание новых энергетических сетей обеспечивающих стабильный источник возобновляемой энергии. Дело, однако, в том, что такие изменения, сколь бы велики они ни были, лишь заменят существующие энергические источники и способы ее передачи, но отнюдь не произведут переворота в энергообеспечении общества, не изменят принципиально роль энергии в нем.

По-настоящему важные социальные изменения в предстоящие два десятилетия произойдут в третьей инфраструктуре по мере того, как слияние воедино технологий телефона, компьютера, факсимиле, кабельного телевидения и видеодисков будет вести ко все более глубокой реорганизации способов коммуникации между людьми, к сокращению, если не к полной ликвидации бумаги в качестве материального носителя информации, к новым способам проведения досуга, к реорганизации образования на основе компьютерного обучения и широкого распространения видеодисков.

Можно скептически относиться к экстравагантным заявлениям о грядущей революции в образовании под воздействием компьютеров и видеомагнитофонов, но как бы

то ни было, в области передачи данных (особенно экономической информации в сфере бизнеса) и развития сетей данных компьюникация вызовет необозримые социальные изменения.

**Социальные и экономические изменения**

Возникает вопрос, какой будет инфраструктура, возникающая вследствие слияния компьютерной и коммуникационной технологий. От становления этой инфраструктуры зависят экономические и социальные изменения, что в свою очередь ставит еще более сложные политические проблемы. Рассмотрим пять центральных проблем в этой области.

Расположение городов. Исторически города формировались на скрещении сухопутных торговых линий, удобно расположенных на местах слияния рек или у больших, хорошо защищенных гаваней на морских и океанских путях. Почти все древние города мира возникли у рек, озер и океанов в те времена, когда транспорт - и особенно водные пути для перевозки тяжелых грузов - начинал связывать различные местности в рамках первой исторической инфраструктуры.

В промышленную эру города возникали вблизи ресурсных баз, в основном угля и железной руды, как это было в Средней Азии, германском Руре или в громадном индустриальном центре США, где сеть озер и рек соединила между собой большие залежи железной руды на севере Миннесоты с громадными залежами угля на юге Иллинойса и западе Пенсильвании. Здесь и возникли великие индустриальные города США - Чикаго, Дейтройт, Кливленд, Буффало и Питтсбург, тесно связанные между собой в громадный комплекс.

По мере перехода к сервисной экономике столичные города становились центрами финансов и управления комплексами предприятий. История Лондона и Нью-Йорка имеет поразительные параллели. Оба города сформировались как порты, через которые шли товары в зарубежные страны или, напротив, в глубь страны. По мере роста торговли здесь в качество вспомогательной деятельности возникали банковское дело, фабричное производство, страховые компании; позже эти города стали центрами финансовых и акционерных соглашений. Что касается конкретно Нью-Йорка, то на третьей стадии своего развития он превратился в своего рода штаб-квартиру корпораций, которых влекли сюда преимущества, связанные с концентрацией в одном месте банковских, юридических, издательских и коммуникационных услуг.

В экономической географии ресурсная база была решающим фактором расположения городов вплоть до последних 40 лет, когда все это начало постепенно меняться. В США после войны экономическая карта страны стала перекрываться преимущественно под воздействием политического фактора, поскольку новые авиационные, космические и ракетные компании создавались исключительно в порядке выполнения правительственных контрактов, и решения относительно того, размещать ли эти компании на северо-западе или на юге Калифорнии, либо на юго-западе Техаса, принимались почти исключительно по политическим соображениям. С развитием грузового авиатранспорта мы стали свидетелями того, что "авиагорода" типа Далласа, Хьюстона, Денвера и Атланты становились региональными центрами, постепенно стягивая к себе промышленную и коммерческую деятельность. А сейчас, когда все более развитые и дешевые телекоммуникации подрывают значение прежней экономики, основанной на факторе географической близости к той или иной ресурсной базе, мы наблюдаем перемещение корпоративных штаб-квартир и сервисных компаний из больших городов, охваченных кризисом, в пригороды.

Местоположение исследовательских лабораторий и новых университетских центров и больших медицинских комплексов все менее зависит от традиционных факторов экономической географии, и все более определяется близостью центров образования, большой политики или же возможностями более свободного образа жизни. Такие феномены, как Долина кремния в Калифорнии - район концентрации электронных и компьютерных фирм вблизи Сан-Хосе - и 128-я магистраль вокруг Бостона, вызваны к жизни близостью

университетских лабораторий плюс к тому удобствами местности, которые не могли предложить небольшим фирмам крупные индустриальные районы.

Сегодня специалисты предсказывают появление "линейных городов", в которых не будет центральных площадей и торговых центров, характерных для классических европейских городов. Б. Ф. Скиннер полагает, что в эпоху развитых коммуникаций нынешние громадные и все менее управляемые города уступят место сетям небольших городов. Оправдаются ли эти прогнозы, неясно: жизнь и смерть городов - это длительный исторический процесс. Что, однако, изменяется, так это сама концепция "урбанизма". 30 лет назад Л. Верт в своем замечательном эссе "Урбанизм как образ жизни" определял урбанизм как в высшей степени интерактивный, мобильный и политически чувствительный образ жизни в противовес жизни в небольшом городке или деревне, зиждущихся на институтах церкви и семьи. Сейчас стремительно урбанизируется вся страна (если не весь мир), при этом все более децентрализуясь в географическом отношении.

Возможности национального планирования. Кем-то сказано, что капиталистическое общество - это общество, в котором каждый заботится только о себе и никто не думает о всех. Что кто-то один может думать о всех - это скорее всего невозможно и даже опасно, так как этот "один" может быть некоей гигантской бюрократией. И все же национальное планирование возможно в следующих вариантах.

- Координация в области информации. Почти все большие предприятия сегодня разрабатывают пятилетние, а то и десятилетние планы по таким показателям, как продукция, капиталовложения, потребности в рабочей силе, в новых помещениях и т. д. Будь у нас создана национальная компьютеризованная служба, можно было бы сводить воедино всю важную информацию такого рода и на ее основе корректировать правительственную и корпоративную политику.
- Моделирование. Используя экономические матрицы входа-выхода - вроде тех, например, какие предложил В. Леонтьев - можно выверять различные альтернативы экономической политики с тем, чтобы в точности уяснить воздействие правительственных решений на те или иные секторы экономики. В еще более радикальном варианте, который предложил советский экономист Л. Канторович, речь идет о создании национальной компьютерной системы, которая, регистрируя различные цены и распределение товаров, помогала бы определять отклонения от запланированных экономических целей и выявлять моменты диспропорционального использования ресурсов в различных секторах экономики.
- Индикативное планирование. В этой модели, которая, к примеру, используется Французским комиссариатом планирования, несколько тысяч отраслевых комитетов координирует свои планы экономической деятельности, и эти скоординированные планы становятся основой для правительственных решений, направленных на стимулирование или, напротив, замедление развития тех или иных отраслей методами кредитной политики.
- Национальные цели. В этой модели правительство ставит ряд национальных целей - например, совершенствование жилищной политики или ускорение темпов экономического роста - и осуществляет общее наблюдение за реализацией этих целей, при необходимости принимая благоприятствующие им меры (налоговые послабления, расширение кредита и т.д.).
- Директивное планирование. Это, в сущности, "военная экономика", воплотившаяся, например, в деятельности Управления по военному производству в США во время второй мировой войны. В этой системе определяются ключевые цели (уровень производства стали, ассортимент машин, численность танков и т.п.), и правительство на основе приоритетов физически распределяет материалы и рабочую силу между соответствующими предприятиями. В данном случае не экономика планируется, а ее ключевые секторы предельно жестко контролируются. Описанные способы планирования варьируются от прямого контроля, с одной стороны, до "элементарной" координации информационной деятельности - с другой. Какой способ планирования больше подходит данному обществу - вопрос политики. При нынешней взаимозависимости и наличии у

решений побочных эффектов некоторая, довольно значительная степень планирования, возможно, просто необходима. Разрабатываемые сейчас компьютерные и коммуникационные системы вполне позволяют осуществлять такое планирование, однако остается весьма сложным вопросом, как совместить его с индивидуальной свободой.

**Централизация и частная сфера жизни**

Сейчас становится все более очевидной угроза полицейского и политического наблюдения за индивидами с использованием изощренной информационной техники. Как писал бывший сенатор С. Эрвин в обзоре по использованию компьютерных банков данных федеральными агентствами, "подкомитет обнаружил многочисленные случаи того, как агентства начинали с весьма благих измерений, а затем столь далеко заходили за пределы необходимого, что неприкосновенность частной сферы жизни и конституционные права индивидов оказывались под угрозой уже в силу самого существования досье на них? Наиболее важным открытием было установление факта чрезвычайно большого количества правительственных банков данных с громадными досье почти на каждого жителя страны. 54 агентства, предоставивших информацию на этот счет, доложили о существовании 858 банков данных, содержащих 1,25 миллиарда записей на индивидов".

Все это элементарно подтверждает один из старейших и до сих пор актуальных трюизмов политики: когда какое-либо агентство, обладающее властью, устанавливает бюрократические нормы и стремится во что бы то ни стало насаждать их, создается угроза злоупотреблений. Другой не менее важный момент заключается в том, что контроль над информацией чаще всего выливается в злоупотребления, начиная с сокрытия информации и кончая ее незаконным обнародованием (и то и другое вполне проявилось в Уотергейте), и что, дабы предотвратить эти злоупотребления, необходимы институциональные ограничения, прежде всего в сфере информации.

**Элита и массы**

Каждое из известных нам обществ делилось по тому или иному осевому признаку на элиту и массы. С другой стороны, общество бывает открытым или закрытым. В прошлом большинство обществ были элитарными и закрытыми в том смысле, что аристократия была чрезвычайно замкнутым сословием. В противоположность этому современные общества стали открытыми, при этом по мере того как знания и техническая компетентность становились непременным условием для входа в элиту, основой процесса для такого продвижения становилось образование. В постиндустриальном обществе элита - это элита знающих людей. Такая элита обладает властью в пределах институтов, связанных с интеллектуальной деятельностью - исследовательских организаций, университетов и т.п., - но в мире большой политики она обладает не более чем влиянием. Постольку, поскольку политические вопросы все теснее переплетаются с техническими проблемами (в широких пределах - от военной технологии до экономической политики), "элита знания" может ставить проблемы, инициировать новые вопросы и предлагать технические решения для возможных ответов, но она не обладает властью сказать "да" или "нет". Последнее является прерогативой политиков, но не ученых или экономистов. В этой связи крайне преувеличенной представляется идея о том, что "элита знания" может стать новой элитой власти.

Что, однако, верно, так это то, что в современном обществе растет эгалитаризм, чему в большой мере содействуют различные группы "элиты знания", особенно молодежной. В целом современное общество состоит из множества образований, вследствие этого появляется и множество элит, так что их координация становится все более сложной проблемой.

**Международная организация**

Сложности создания новой инфраструктуры коммуникаций в национальном масштабе велики, еще более сложный характер соответствующие проблемы приобретают в международном плане. В последние 30 лет Соединенные Штаты стали "национальным обществом", в ближайшие же 20 лет будет идти процесс становления международного

общества, но не в виде организованного международного порядка, а в виде некоей пространственно-временной целостности, обусловленной глобальностью коммуникаций. Проблема, однако, заключается в отсутствии какой-либо политической основы для международно-правового оформления и организации международной инфраструктуры.

Сейчас объем международных телефонных переговоров растет на 20% ежегодно. Эта международная связь осуществляется Интелсатом - международной коммерческой организацией, охватывающей 90 с лишним стран-членов. Однако Интелсат зависит от американской аэрокосмической компании "Хьюс эйркрафт" в том, что касается производства спутников, и от американского аэрокосмического агентства в том, что касается их запуска на орбиту. Гегемония США в этой области не может не стать острейшей политической проблемой в ближайшие десятилетия.

Важной проблемой становится необходимость создания глобальной сети банков данных и услуг: все больше и больше стран со своими научными, техническими и исследовательскими организациями стремятся получить доступ к компьютеризованным системам, разработанным в развитых индустриальных обществах.

**Поворотные пункты и перспективы**

Я стою на том, что информация и теоретическое знание суть стратегические ресурсы постиндустриального общества. Кроме того, в своей новой роли они представляют собой поворотные пункты современной истории.

Первый поворотный пункт - изменение самого характера науки. Наука как "всеобщее знание" стала основной производительной силой современного общества.

Второй поворотный пункт - освобождение технологии от своего "императивного" характера, почти полное превращение ее в послушный инструмент. Современная технология открывает множество альтернативных путей для достижения уникальных и вместе с тем разнообразных результатов, при этом неимоверно возрастает производство материальных благ. Таковы перспективы, вопрос лишь в том, как их реализовать.

**Источник:** http://www.nethistory.ru/biblio/1043172230.html (14.10.2011)

*А.А.ЧЕРНОВ*

# ОСНОВНЫЕ ИСТОРИКО-ТЕОРЕТИЧЕСКИЕ ЭТАПЫ РАЗВИТИЯ КОНЦЕПЦИЙ ГЛОБАЛЬНОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА

Развитие системы дорог и судоходства привело в свое время к становлению мирового торгового рынка. Появление и широкомасштабное использование радио, телефона и других средств коммуникаций первой половины минувшего века сделало возможным формирование транснациональной индустриальной экономики и индустриального общества. Залогом успешного развития современной экономики и общества стали информационные и телекоммуникационные технологии, разнообразие и возможность применения которых, как показывает практика, ограничены лишь изобретательностью самого человека.

В настоящее время информационно-коммуникационные технологии переживают процесс ускоренного развития. Если раньше этот процесс протекал в направлении четко определенной специализации и дифференциации, то сегодня ситуация принципиально изменилась: главным условием, которому технологии должны соответствовать, является возможность их универсального использования. Это требование нашло отражение в мультимедийных системах, способных объединять функции, например, телевизора и радиоприемника, фотолаборатории и виртуальной библиотеки, телефона и факса, обеспечивая при этом классический набор вычислительных функций и быстрый доступ к сети Интернет.

Можно с полной уверенностью говорить о том, что одним из важнейших катализаторов этого процесса явилось мировое признание компьютерной сети Интернет. Именно она смогла объединить миллионы людей и сотни стран, сократить географические расстояния и ликвидировать преграды для общения в различных областях деятельности человека. Следует отметить, что многократно испытанные преимущества Интернет практически во всем мире привели к массовому отказу, несмотря на уже произведенные многомиллиардные вложения, от развития собственных корпоративных или ведомственных сетей в пользу построения открытых стандартизованных систем и их интеграции в Интернет.

Появление сети и начавшаяся по всему миру либерализация рынка, следствием которой стало соответствующее снижение стоимости коммуникационных услуг, - два основных фактора, которые сыграли определяющую роль в развитии информационной сферы, усиления ее социального аспекта. Последующее 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 результатам проведенного министерством торговли США исследования, радио понадобилось 30 лет, чтобы достичь аудитории в 50 млн. человек, телевидению - 13 лет, а Интернету - всего 4 года.[1]

Наблюдаемый прогресс информационно-коммуникационных технологий открывает огромные возможности всем частным лицам, компаниям и сообществам более эффективно и творчески решать насущные экономические и социальные проблемы. Электронная коммерция и телеработа, дистанционное образование и телемедицина - вот, далеко не все направления внедрения и непосредственного использования сегодня новых информационных технологий. Но особенно важным моментом является то, что с интенсивным развитием самих глобальных сетей совершенствуется и появившаяся возможность непосредственного общения между людьми различных народов и государств в режиме реального времени. Именно этот фактор оказывает возрастающее влияние на политику, экономику, культуру государств мира и международные отношения в целом.

Таким образом, современные достижения в информационной сфере носят поистине революционный характер и создают предпосылки для движения к совершенно новому типу

[1] Министерство торговли США сообщает…//Мир Internet, 1998, № 6.

общества XXI века - информационному, или, как его еще называют, обществу знания. Одной из основополагающих характеристик информационного общества является его глобальный характер. Сегодня мы являемся свидетелями того, как в ходе его становления постепенно стираются границы между странами и людьми, радикально меняется структура мировой экономики. Подобные принципиальные изменения, вызванные стремительным развитием информационных и телекоммуникационных технологий, стали предметом особого внимания ученых, политиков, специалистов в информационной сфере.

Изучение вопросов наметившихся глобальных перемен с целью выработки соответствующих рекомендаций и программ, позволивших бы ускорить формирование глобального информационного общества, имеет богатые традиции в русле концепций постиндустриализма. Среди зарубежных авторов, занимающихся этими проблемами, следует отметить работы Д.Белла, И.Масуды, Т.Стоуньера, М.Постера, Р.Катца, Д.Рисмана, Х.Шрадера, Д.Тапскотта, М.Маклюэна, Э.Тоффлера, П.Дракера, М.Кастельса, М.Бангеманна, Д.Лайона, Дж.Мартина и других. Отечественная наука здесь представлена трудами И.Н.Курносова, А.И.Ракитова, О.А.Финько, Ю.М.Нестерова, А.Б.Артамонова, А.В.Петрова, Е.И.Орлова, О.В.Кедровского, С.А.Дятлова, Г.Л.Смоляна, Д.С.Черешкина.

Поскольку в рамках данной статьи рассмотреть исследования и изложенные в них точки зрения всех вышеперечисленных авторов представляется практически невозможным, остановимся лишь на некоторых из них, необходимых для того, чтобы попытаться выделить основные этапы развития идей и концепций глобального информационного общества.

Понятие «информационное общество» появилось во второй половине 1960-х годов. Изобретение самого термина «информационное общество» приписывается профессору Токийского технологического института Ю.Хаяши. Впервые основные характеристики общества знания 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» (1969г.), «План информационного общества» (1971г.).[2] В перечисленных отчетах высокоиндустриальное 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 коснуться 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 социологии и 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 информационно-телекоммуникационных технологий, 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.

Второй этап в развитии идей глобального информационного общества начинается с выходом в 1973 году книги американского социолога Д.Белла «Грядущее

[2] Алексеева И.Ю. Возникновение идеологии информационного общества//Информационное общество, 1999, № 1, с. 30-35.

постиндустриальное общество. Опыт социального прогнозирования».[3] 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 и другим теоретикам индустриализма, он трактует индустриальное общество как общество, в котором главной целью ставится производство максимального числа машин и вещей. Существенной чертой постиндустриального стадии является, по мнению Д.Белла, переход от производства вещей к развитию производства услуг, связанных с образованием, здравоохранением, исследованиями и управлением.

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».[4] 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.

Данная книга вызвала не только всеобщий резонанс и интерес к затронутой в ней проблематике, но и в значительной степени обусловила появление и ряда других концепций глобального информационного общества. 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 композиции грядущего общества представлены в его книге «Информационное общество как постиндустриальное общество».[5] 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 развитие сотрудничества. Ведущей отраслью экономики станет интеллектуальное производство, продукция которого будет аккумулироваться и распространятся с помощью новых телекоммуникационных технологий.

Уделяя особое внимание трансформации человеческих ценностей в глобальном информационном обществе, И.Масуда предполагает, что оно будет по сути бесклассовом и бесконфликтным, - это будет общество согласия с небольшим правительством и государственным аппаратом. Он пишет, что в отличие от индустриального общества, характерной ценностью которого является потребление товаров, информационное общество выдвигает в качестве характерной 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

[3] Bell D. The Coming of Post-industrial Society. A Venture in Social Forecasting. N.Y., Basic Books, Inc., 1973.
[4] Там же, p. 20.
[5] Masuda Y. The Information Society as Postindustrial Society. Washington.: World Future Soc., 1983.

информации.[6]

По мере развития электронных средств массовой информации и информационных технологий в науке 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 концепции, представленные ими в своих исследованиях получили как весьма положительные, так и далеко не лестные оценки со стороны традиционной науки и общественности в целом.

Отличительной особенностью взглядов М.Маклюэна является то обстоятельство, что информационные технологии 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.

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».[7] 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 на дому и «электронные коттедж». 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, оснащенной «умной» печатной машинкой, а может быть, еще и копировальной машиной или компьютерным пультом и телекоммуникационным устройством, то возможности организации работы на дому резко возрастут».

Сегодняшнее положение дел в этой области показывает, насколько прав оказался Тоффлер в своих суждениях. Речь идет о развитии т.н. «дистанционных» трудовых отношений, называемых иначе «телеработой» или «телекомпьютингом». Согласно некоторым данным, уже в 1997 году численность телерабочих в Европе составила более 2 млн. человек, а в США - около 11 млн. Есть оценки, что в 2002 году около 20 % рабочей

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

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

силы будут пользоваться теледоступом.[8] Основные социально-экономические преимущества массового применения средств телеработы таковы: уменьшение транспортных проблем, общих передвижений и связанных с этим загрязнений окружающей среды; возможность получить работу практически в любой точке мира, что, в свою очередь, снижает уровень общей безработицы; расширение возможностей трудоустройства людей с ограничениями по здоровью, например, не позволяющими им передвигаться. С помощью новых информационных технологий последние также могут полноценно работать, обучаться и общаться.

Рубеж 1980/90-х годов можно обозначить как начало нового этапа в развитии концепций 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 активное участие еще в дискуссиях начала 70-х годов. Однако свой непосредственный вклад в формирование нового облика существующих концепций постиндустриализма он внес позднее, опубликовав книгу «Посткапиталистическое общество».[9] 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 экономики и социума. Современная эпоха, по мнению Дракера, представляет собой время радикальной перестройки, когда с развитием новых информационно-телекоммуникационных технологий 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».[10] Исходя из того, что информация по своей природе является таким ресурсом, который легче других проникает через 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 Кастельс неоднократно обращает внимание читателя на существенное различие между уже существующими концепциями информационного общества (Information Society) и его собственной концепцией «информационального общества» (Informational Society). В концепциях информационного общества подчеркивается определяющая роль информации в обществе. По мнению автора, информация и обмен информацией сопровождали развитие цивилизации на протяжении всей истории человечества и имели особое значение во всех обществах. В то же время зарождающееся «информациональное общество» строится таким образом, что сбор, анализ и передача необходимой информации стали «фундаментальными источниками производительности и власти».

За последнее десятилетие к теме глобального информационного общества неоднократно обращались и отечественные ученые, которые разработали собственные определения и концепции формирования нового общества. Так, А.И.Ракитов в работах конца 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,

[8] Status Report on Telework. – http://www.eto.org.uk/twork/tw97eto/
[9] Дракер П. Посткапителистическое общество. СПб., 1999.
[10] Кастельс М. Информационная эпоха: экономика, общество и культура. М., 2000.

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.[11] С учетом этого, развитие, прежде всего, данного сектора позволит значительно ускорить интеграцию отдельно взятой страны в глобальное информационное общество.

Г.Л.Смолян и Д.С.Черешкин в разработанной ими концепции к основным признакам нового общества относят: формирование единого информационного пространства и углубление процессов информационной и экономической интеграции стран и народов; 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.[12] Вместе с тем 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 Никита 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, хотя это жизненно важно для всех остальных. Необходима смена шкалы ценностей и менталитета. «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».[13]

Одной из принципиально важнейших характеристик данного периода является то, что, начиная с первой половины 90-х годов, большинство американских и европейских исследователей и специалистов в этой области стали акцентировать внимание на роли и значении не столько самой информации в различных сферах жизни, сколько знаний, что, в свою очередь, породило целый ряд новых определений высокоиндустриального общества, среди которых такие, как «Knowledge Society», «Knowledgeable Society» и т.д. Другая, не менее важная, особенность заключается в том, что стремительный рост информационных систем и ускоряющееся развитие электронных сетей, связанных между собой и пересекающих традиционные национальные, политические и экономические границы, привели к вынужденному изменению направления политической мысли. Политики прочувствовали необходимость планирования предстоящего развития информационных технологий, которые, как выяснилось, могут оказать как позитивное влияние на общество, так и негативное.

---

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

[12] Черешкин Д.С., Смолян Г.Л. Сетевая информационная революция//Информационные ресурсы России,1997, № 4, с. 15-18.

[13] Моисеев Н. Информационное общество как этап новейшей истории//Свободная мысль, 1996, № 1, с. 81-83.

В 1993 году вице-президент США А.Гор использовал понятие “информационная супермагистраль”, а вскоре после этого на конференции Международного союза телекоммуникаций он говорил уже о глобальной информацинной инфраструктуре. В предложенной концепции развития информационного общества последнее описывалось им следующим образом: учебные заведения и преподаватели становятся доступными всем студентам, вне зависимости от географических условий, расстояния и ресурсов; огромный потенциал искусства, литературы и науки становится доступен не только в библиотеках и музеях; медицинские и социальные услуги становятся доступными в интерактивном режиме; каждый имеет возможность полноценно работать через электронные магистрали, обращаться в магазин, банк, получать государственную информацию прямо из своего дома; деловые структуры могут обмениваться информацией электронным путем, снижая объем бумажного документооборота и улучшая качество услуг.[14] С этого момента развитие национальной и глобальной информационной инфраструктуры становится стратегической целью государства.

Вслед за США в разработку данной проблематики активно включились страны Западной Европы, в которых идеи глобального информационного общества также сравнительно быстро нашли своих сторонников. В выпущенном в декабре 1993 года Комиссией Европейского сообщества докладе «Рост, конкурентоспособность, занятость – вызовы XXI века и пути в него» подчеркивалось, что информационное общество обладает существенным потенциалом, способствующим устойчивому развитию, росту конкурентоспособности, увеличению рабочих мест, улучшению качества жизни каждого европейца.

В июле 1994 года КЕС был принят план действий «Европейский путь в информационное общество» (Europe′s Way to the Information Society. An Action Plan)[15], который предусматривал четыре основных направления деятельности Европейского Союза: создание нормативно-правового пространства; развитие информационных и телекоммуникационных сетей, классификация основных услуг, стандартизация оборудования; изучение различных социальных и культурных аспектов информационного общества; пропаганда концепции формирования информационного общества среди населения с целью заручиться общественной поддержкой. План действий часто называют «Инициативой Бангеманна» по фамилии одного из руководителей Комиссии Европейского сообщества, который возглавил группу высокопоставленных экспертов, подготовивших рекомендации Комиссии о принятии срочных мер для обеспечения вхождения стран ЕС в информационное общество. М.Бангеманн был обеспокоен, главным образом, тем, как бы европейские страны не оказались в фарватере других стран, занимающих лидирующие позиции в мире по производству вычислительной техники и новых технологий.

В ответ на появление «Инициативы Бангеманна» во многих странах мира (Германия, Франция, Великобритания, Австрия, Чехия, Япония, Индия, страны Юго-Восточной Азии и в других) началась разработка и реализация национальных концепций развития информационного общества. В частности, в 1995 году Финляндия подготовила свою программу «Финский путь в информационное общество», в феврале 1996 года в правительство ФРГ была представлена программа действий «Путь Германии в информационное общество». Основные задачи, сформулированные в концепциях, видятся в следующем: улучшить условия для бизнеса с помощью эффективной и согласованной либерализации телекоммуникаций, создать необходимые условия для внедрения электронной торговли; обеспечить переход к обучению в течение всей жизни путем реализации инициативы «Обучение в информационном обществе»; осознавая важность глобального сотрудничества, установить правила построения информационного общества, которые должны затрагивать права на интеллектуальную собственность, защиту данных и

[14] Курносов И.Н. Информационное общество: планы и программы зарубежных стран. М., 1997.

[15] Улла Скиден. Глобальный вызов Бангеманна: о международной программе Европейской комиссии по интеграции городов в информационное общество//Информационное общество, 1999, № 4, с. 11-12.

тайну личной жизни, распространения вредного и незаконного содержания, а также проблемы налогообложения в электронной сфере.

Поскольку для большинства европейских стран проблема приватизации уже решена, дискуссии в настоящий момент идут о политике либерализации телекоммуникаций, которая до сих пор остается одним из самых острых вопросов, обсуждаемых на международном уровне. Лидирующие позиции в процессе либерализации занимают Великобритания, Швеция, Финляндия, Нидерланды. Во Франции эта проблема старательно игнорируется, поскольку она не согласуется с французским планом централизованного развития инфраструктуры информационного общества. В Дании либерализация идет с большой скоростью, однако, эта проблема не относится к числу приоритетных направлений.[16]

Другой, не менее актуальной проблемой, является вопрос, что следует развивать сначала: сети или услуги. Разные страны по-разному отвечают на него. К примеру, в шведской концепции развития информационного общества эта проблема даже не поднимается, речь идет лишь об услугах. В датской и голландской она не является значимой, а вот в английской и французской концепциях проблема “сети или услуги” становится центральной: в этих документах указывается, что именно строительство сетей - путь к развитию сферы услуг. Следует также отметить, что практически всеми программами ставится целью развитие “универсального обслуживания”. Причиной этому служит серьезная озабоченность стран, связанная с проблемой неравенства в информационном обществе, когда большая часть населения может просто оказаться за его бортом.

Азиатские концепции развития информационного общества, как правило, базируются на утверждении собственных ценностных ориентаций и стремлении разработать альтернативный западному подход к индустриализации и социальному развитию. В их основе лежат сотрудничество государства и рынка, попытка установить связь между культурными ценностями, свойственными конфуцианству, и происходящими социальными изменениями.[17] Философские постулаты «сосуществования» и «сопроцветания», а также содействие государства в реализации этих принципов на уровне отдельной организации - вот, по мнению, азиатских специалистов, залог удачи.

В результате, успехи Японии в развитии информационного общества сопоставимы сейчас, пожалуй, с успехами США. Одним из важнейших факторов их достижения всегда были и до сих пор остаются значительные расходы на научные исследования и разработки, высокий приоритет информационно-коммуникационных технологий в обеспечении социально-экономического развития страны. На сегодняшний день ее главным приоритетом становится собственное производство нового знания, новых технологий и продуктов, а в центре внимания - новаторские идеи, точки зрения и оригинальность. Известно, что для страны из-за низкой рождаемости характерно сегодня старение населения. Есть надежда, что за счет новейших информационных технологий удастся в какой-то мере компенсировать отрицательное влияние на экономику уменьшения численности трудоспособного населения.

В основе информационного развития “азиатских тигров” (Южная Корея, Тайвань, Сингапур и Гонконг) лежит так называемая концепция экономического сотрудничества государства и рынка. Успех этих стран базируется, в частности, на вмешательстве государства в принятие решений в области крупных вложений частного капитала, на его активном участии в создании материальной, социальной и информационной инфраструктур. Основными вопросами информационного развития, по которым правительства высказывают особую озабоченность, являются сегодня постоянно растущая конкуренция в области производства и внедрения новейших информационно-коммуникационных технологий, связанная с этим потенциальная возможность потери какого-то сегмента рынка или рабочих мест. Особого внимания среди “тигров” заслуживает Сингапур, разработавший

[16] Вершинская О.Н. Существующие модели построения информационного общества//Информационное общество, 1999, № 3, с. 54.
[17] Там же, с. 55-57.

стратегический план “Интеллектуальный остров”.[18] Его намерения состоят в том, чтобы “стать одной из первых стран в мире с развитой национальной информационной инфраструктурой, обеспечивающей связь компьютеров практически в каждом доме, школе или рабочем месте”.

Индия не выбрала ни пути полной приватизации, ни мягкой либерализации, ее концепцию можно назвать промежуточной. Государственные предприятия не передаются в частный сектор, но конкуренция разрешается на рынке местных услуг, при этом допускается 49 % иностранного присутствия (в стране более 200 млн. семей со средним доходом, так что внутренний рынок весьма перспективен).[19] Своим главным капиталом на пути в глобальное информационное общество Индия считает свои человеческие ресурсы. На сегодня она имеет третий по величине (после США и России) научно-технический потенциал в мире и относительно хорошую законодательную систему. Другими особенностями данной концепции являются осторожность и постепенность, а также опора на национальные культурные корни.

Активным участником процесса формирования информационного общества является и Россия. В стране создаются и внедряются новейшие информационные и телекоммуникационные технологии, используются уникальные информационные ресурсы, естественным образом формируется культура, порождаемая информационной эпохой.

К примеру, на протяжении последнего времени наблюдается динамичное развитие российского сегмента глобальной информационной сети Интернет. По оценкам различных независимых исследовательских агентств (Комком-2, ФОМ, РОЦИТ), на сегодняшний день приблизительно 7 млн. россиян хотя бы один раз использовали Интернет для работы или развлечения. Число людей, постоянно работающих в сети, превышает 3 млн., а к 2010 году может составить около 26 млн. Для сравнения: в США, по данным Strategis Group, уже в ноябре 1999 года число пользователей достигло 100 млн., что составляет примерно 50 % от общей численности населения. Быстро растет количество российских Web-сайтов: их число на русском языке (собственно Web-сайтов и отдельных крупных информационных разделов) составляет на текущий момент более 6 тысяч. Большой популярностью в стране пользуется бесплатное программное обеспечение (27%), компьютерные игры (22,7 %) и развлечения (22,5 %).[20]

В целом по общему объему информационных ресурсов Россия занимает весьма достойные позиции в мире, однако, их качество и структура, а также степень использования, к сожалению, отстают от современных потребностей. Согласно статистике, ситуация следующая: подавляющее большинство существующих данных хранится в автономных, как правило, изолированных информационных системах и недоступно через Интернет, а баз данных, доступных для широкого круга пользователей, насчитывается около 3 тысяч. Как показывает практика, средний объем и срок жизни большинства российских баз данных существенно уступают зарубежным аналогам. Из всех баз данных, имеющихся в России, только 16% способны функционировать в режиме удаленного доступа, причем, половина из них находится в Москве и Санкт-Петербурге.

Вместе с тем в стране активно формируется рынок электронной информационной продукции и услуг, в котором основную роль играют негосударственные структуры, быстрыми темпами развивается индустрия мультимедиа. Начав с русификации широко применяемых зарубежных программных продуктов, многие фирмы успешно перешли к созданию и распространению оригинальных программ, ориентированных на российского пользователя. Сегодня значительная доля программно-технического обеспечения процессов информатизации и развития телекоммуникаций обеспечивается российским

[18] Singapores Vision of an Intelligent Island. - hppt://128.100.159.139/FIS/Res/Pub.IT2000.html
[19] Вольф М. Народный компьютер по-индийски//PCWeek, 2000, № 7.
[20] Интернет в России: стратегические данные и социальный состав пользователей (Департамент правительственной информации Аппарата Правительства РФ) – http://www.e-government.ru/pub/stat/985431649.html

информационным рынком, на котором все новейшие средства и технологии предоставляются практически одновременно с их появлением на зарубежных рынках.

В настоящее время на территории России действует более 40 федеральных законов в области информации, более 80 актов президента, около 200 актов правительства Российской Федерации. В частности, существует Концепция государственной информационной политики, разработанная в 1998 году, Концепция формирования информационного общества в России, одобренная Государственным Комитетом РФ по связи и информатизации в мае 1999 года, Доктрина информационной безопасности Российской Федерации, утвержденная Президентом России В.В.Путиным 9 сентября 2000 года.[21]

Основой российского пути интеграции в глобальное информационное общество, по мнению авторов, должно стать расширение и углубление информатизации всех сфер жизни, ориентация общественного сознания на особенности жизни в информационном обществе, формирование рынка информационных продуктов и универсальных информационных услуг, обучение разных категорий населения умению получать и эффективно использовать информацию.

Анализ состояния и тенденций развития процессов информатизации и компьютеризации в России показывает, что стране в целом на сегодняшний момент удалось достичь значительных успехов в развитии национальной информационно-телекоммуникационной инфраструктуры. Но этот вывод, хотя и опирается на ряд, безусловно, позитивных показателей и фактов, не означает, что решены все основные проблемы и устранены главные препятствия на пути информатизации. Предстоит еще многое сделать.

Все вышесказанное позволяет выявить общие признаки и обозначить основные положения существующих концепций развития глобального информационного общества, сочетающих в себе как философские, так и прикладные аспекты:

- обобщая рассмотренные подходы к трактовке понятия «глобальное информационное общество», можно сказать, что в настоящее время под таковым понимается: общество нового типа, формирующееся в результате новой глобальной социальной революции, основой которой является взрывное развитие и конвергенция информационных и коммуникационных технологий; общество знания, в котором главным условием благополучия каждого человека и каждого государства становится знание, полученное благодаря беспрепятственному доступу к информации и умении с ней работать; общество, которое, с одной стороны, способствует взаимопроникновению культур, а с другой, открывает каждому сообществу и человеку новые возможности для самоидентификации;

- при разработке концепций перехода к информационному обществу, как правило, используется комплексный подход, основанный на поддержании баланса интересов государства, общества, предпринимательских структур и личности;

- поскольку формирование глобального информационного общества происходит, прежде всего, под воздействием прогресса новых информационных и телекоммуникационных технологий в сочетании с глобализацией рынков как внутри отдельно взятой страны, так и на международной арене, то для гармоничного вхождение в информационное общество и соблюдения требуемого баланса необходимы координирующие усилия со стороны государства как органа, способного наиболее полноценно выразить и обеспечить интересы всего общества.

При этом необходимо не забывать, что главная цель построения глобального информационного общества - улучшение жизни людей, создание условий для их максимальной самореализации - может быть достигнута лишь при соблюдении ключевого принципа: любое развитие должно опираться не на объекты, а на людей.

**Источник:** http://www.isn.ru/public/is.doc (17.10.2011)

[21] Бачило И.Л. Потенциал законодательства в процессах становления информационного общества//Информационное общество, 1999, № 3, с. 40-43.

*Д.Н. ПЕСКОВ*

# ИНТЕРНЕТ В МИРОВОЙ ПОЛИТИКЕ И МЕЖДУНАРОДНЫХ ОТНОШЕНИЯХ

Распространение Интернета во второй половине 1990-х гг. в большинстве стран мира создало условия для организации на современном пространстве принципиально новых способов коммуникации, равно приложимых в политике, науке, бизнесе, повседневном общении и развлечении. Сеть стала сильнейшим стимулятором для традиционных структур, обеспечивающих воспроизводство вышеперечисленных сфер. Начав с микроуровней политического, Интернет очень быстро вырос в важный фактор мировой политики, средство формирования глобального общества, раздражитель и объект международных отношений.

В многообразии форм, связывающих Интернет и мировую политику, значимую роль играют характеристик контекста, в котором проходит эволюция последних. Очевидно, что сегодня мы наблюдаем лишь первые проявления будущего общества с чертами современности, отличающимися от сегодняшних.

Во время своем зарождения Интернет был прежде всего технологией, способом и типом коммуникации. Исторический опыт человечества показывает тесную зависимость между появлением новых видов коммуникации и политико-социальной организацией общества. Возникновение письма, колеса, телеграфа, железной дороги, телефона, радио, телевидения каждый раз меняло политическую организацию общества. При одновременном воздействии нескольких новшеств изменения происходили еще скорее. Признавая Интернет изобретением, как минимум равнозначным телефону или радио, а в пределе соглашаясь с пришествием Природы-2 или, вслед за некими лингвистами, начало третьего этапа после речи и письма, мы должны ожидать не менее масштабных изменений в устройстве общества XXI в.[65] Со времени внедрения Всемирной Паутины в повседневную жизнь прошло менее десяти лет, а принципиальные изменения в ее структуре, продолжающие повышать эффективность и скорость коммуникации в любом масштабе измерения происходят быстрее, чем это отслеживают аналитики. Система Интернет - общество находится в постоянном развитии. Инертность политических преобразований в традиционных структурах значительно выше, чем аналогичные изменения в интернет-пространстве. При невозможности теоретического анализа интернет-процессов в реальном масштабе времени, мы вполне способны отслеживать перемены в «обществе офлайна».

Сам по себе Интернет - сложный феномен, не сводимый к любому одному определению. У него множество граней, включающих в себя технические, социальные и политические характеристики явлений. Здесь и далее под терминами «интернет-пространство», «Интернет» мы будем понимать *совокупность сетевых отношений, социальных институтов, технологий и технических средств*, связанных внутри себя и друг с другом с помощью *компьютерно-опосредованных линий*, а также характеризуемых *единым временем и пространством с особыми характеристиками*.

В таком расширенном толковании Интернет включает в себя социальную действительность, претендуя не только на виртуальность, но и на часть традиционно понимаемом «реальности», в т.ч. на совокупность сетей гуманитарных, социальных и технологических. Едва тот или иной социальный либо политический институт внутренне

---

[65] Технологические революции второй половины XX в., сменяя друг друга, перешли сегодня в стадию непрерывного экспоненциального роста, приближаясь к точке перелома. Такой рост не может длиться бесконечно, и за многочисленными новшествами в технологиях последуют не менее масштабные социальные изменения. Новые технологии коммуникации позволяют создать принципиально иные социальные формы. Они уже появились на уровне Интернета и неизбежно возникнут в повседневном мире, как только большинство общества будет способно эффективно использовать возможности коммуникации XXI в.

Сверх того, единственным ограничителем беспрерывного технологического роста могут явиться лишь новые социальные образования. Значит, их роль вполне диалектична: она объективно обусловлена необходимостью лимитации технологического роста и его рисков, в то время как новые социальные формы - прямое следствие технологической революции, ибо прежние институты такого рода не в состоянии адекватно реагировать на всесторонние неупорядоченные вызовы.

задействуют сетевой принцип коммуникации на основе технологий, которые включают его в общемировое пространство с едиными законами времени и пространства, а сетевое существование становится основой деятельности данной организации, она входит в интернет-пространство. Помимо «физических» различий, сетевая организация подразумевает иное предназначение личности в организации, иную политическую роль отдельного человека. Предельным требованием к сетевой эффективности является возможность получения и распространения информации, включая информационное действие, в любом месте в любое время в любом объеме. При достижении данного критерия отдельный участник сети получает в свое распоряжение все ресурсы данной сетевой организации, то есть становится ей равен. Фактически, предельно усложненная сеть, интернет, делает равным индивида и любое государство. Итак, сетевой организацией может называться организация, которая дает своему члену возможности любого другого политического субъекта. В этом смысле понимание Интернета исключительно как технического средства коммуникации или совокупности компьютеров и проводов устарело, мешает обществу осознать и использовать возможности кибер-пространства.

Интернет охватывает всю область политических коммуникаций в современном социуме, видоизменяя и устанавливая их новые принципы. При этом ценность интернета повышается в квадратичной пропорции по отношению к числу узлов в интернете (т.н. «Закон Меткафа»). На практике это означает, что при росте числа пользователей интернета с 500 миллионов до одного миллиарда ценность интернета и его возможностей возрастет в четыре раза.

Современное состояние интернет-пространства, заложенные в нем политические принципы во многом обязано истории появления и развития технологий, положивших начало интернету. В начале 1960-ых годов прошлого века руководство США было крайне обеспокоено отставанием от СССР в военно-технической гонке. Территория США была практически беззащитна перед угрозой применения советских баллистических ракет с ядерными зарядами. Для ликвидации отставания в гонке вооружений и, в частности, обеспечения стратегической управляемости США в случае ядерной войны в США создается Агентство перспективных проектов (Advanced Research Project Agency (ARPA, затем DARPA). Одним из первых проектов агентства становится разработка новой устойчивой архитектуры управления компьютерными центрами. Теоретическое решение данной задачи состояло из трех основных принципов, которые стали основой интернета: каждый узел сети был соединен с другими так, что от него вело несколько каналов информации; при этом каждый узел сети рассматривался как потенциально уязвимый; информация передавалась пакетами, которые в случае обрыва связи или уничтожения соседнего компьютера перенаправлялись по любому другому доступному каналу. Таким образом достигалась управляемость системы. Как предположили аналитики RAND, (представители научных кругов отрицают изначальное военное предназначение сети) в случае ядерной атаки, уничтожение одного или нескольких командных центров позволяло сохранить военную инфраструктуру управляемой и нанести ответный удар. Путь к действительному созданию такой системы оказался достаточно долгим. В августе 1962 года исследователь Массачусетского технологического института Дж. Ликлайдер предложил концепт «Галактической сети» (Galactic Network), в октябре он же возглавил исследовательскую компьютерную группу DARPA. К 1968 году, с учетом параллельных исследовательских проектов в корпорации RAND и других организациях, США вплотную подошли к созданию первой компьютерной сети, получившей название ARPANET. 1968 год был богат на события, впоследствии повлиявшие на современное состояние интернета и общества в целом. События касались социальной, технологической и научной сфер человеческой жизни. Студенческие революции 1968 года, «красный май» в Париже ознаменовали наступление эпохи социального постмодерна. Скандальные лозунги парижских улиц буквально через 10-15 лет стали лозунгами западного общества с его характеристиками толерантности, иронии, сексуальности, цинизма, всеобщего смешения жанров и симуляции действительности. Не

менее значимыми, хотя и менее заметными были изменения в науке и технологии. В 1969 году в США появляется прообраз современного интернета – военная сеть ARPANET. Третьим событием, которое оказывается объектом нашего внимания, становится введение профессором Токийского технологического института Хаяши в научный оборот понятия «информационное общество». В 1969 году Агентство экономического планирования EPA (Economic Planning Agency) представляет доклад "Японское информационное общество: темы и подходы" ("Japan's Information Society: Themes and Visions". Два первых события порождают тенденции, которые приводят к торжеству постмодернизма в современном мире, в том числе в мировой политике и международных отношениях, и к созданию глобальной информационной системы интернета. Научная тенденция изучения проблематики «информационного общества» с каждым годом все более отклоняется от первых двух тенденций. Сеть ARPANET быстро развивается, в 1972 году по ней отправляется первое электронное письмо, и в начале 1980-ых годов происходит судьбоносная для интернета передача технологий ARPANET из военного в гражданский сектор. Такое решение, совпавшее по времени с быстрым распространением персональных компьютеров в США, приводит к созданию первой сети с потенциалом глобального распространения – сети Usenet. К 1984 году относится и первое появление в сети Usenet политического сообщения из Советского Союза – по всей видимости, фальшивки, написанной от имени Константина Черненко. В послании, якобы отправленном из МГИМО, лидер советского государства разъясняет основы политики мирного сосуществования и призывает пользователей Usenet вместе бороться за мир во всем мире. Необходимо отметить, что на развитие как интернета, так и всей компьютерной индустрии в целом сильное влияние оказали движения фрикеров (взломщиков телефонных сетей) и хакеров (взломщиков компьютерных систем). Так, фрикерами были создатели корпорации Apple Стив Джобс и Стив Возняк. Сеть быстро распространяется (преимущественно в университетской среде) за пределы США, и к 1990 году достигает территории СССР. В Европе существовали альтернативные проекты компьютерных систем, некоторые из которых достигали общенационального охвата (крупнейшей была сеть Minitel во Франции), но по разным причинам они не получили такого развития, как Usenet, FIDOnet и впоследствии интернет. В СССР развитие интернет-технологий не осталось вне поля зрения государственных и академических организаций. В конце 1980-ых годов велись активные разработки аналогичной системы связи для стран СЭВ, однако выбранный курс на разработку системы «с нуля», и ограниченность области применения компьютерных технологий в рамках советской административной системы, привели к тому, что о разработках забыли немедленно после распада СССР. Собственно интернет остался вне внимания государства. В 1990 году регистрируется домен высшего уровня SU, первоначально принадлежащий студенту из Хельсинки, представлявшему интересы кооператива «Демос». Во время событий августа 1991 года каналы «Демоса» используются для передачи данных о действиях вокруг Белого дома в Европу и США, и, таким образом, интернет впервые становится фактором мировой политики, получив распространение на территории подавляющей части земного шара. В начале 1990-ых годов появляется технология www (world wide web), первый графический браузер (средство просмотра веб-страниц) Mosaic, и интернет фактически приобретает современное состояние.

*Сегодня международная система интернет-пространства* состоит из трех основных частей, обеспечивающих функционирование современного Интернета[66].

1.Системы *доменов* и *доменных адресов*, определяющих символическое положение веб-сайтов в интернет-пространстве, его топологию. Домены делятся на общие (com, net, org, biz, edu) и национальные (ru, uk, fr…). Для наших целей важно понимать, что система доменов поддерживается только согласием основных провайдеров, предоставляющих услуги доступа в Интернет. Они добровольно соглашаются следовать стандартам сетевых организаций, управляющих структурой Интернета: IAB (англ. Internet Architecture Board), IETF (Internet

[66] Мы говорим о *современном* Интернете, так как аналогичная сеть, скажем, 2010 г. будет не в меньшей степени базироваться на интеллектуальных семантических агентах, почти отсутствующих сегодня.

Engineering Task Force), ICANN (International Corporation for Assigned Names and Numbers) и Internet Society (ISOC). Ведущая роль в управлении Интернетом принадлежит ICANN, которая контролирует значительную часть доменного пространства и структуру интернет-протоколов. Организация была создана в 1998 г. по решению правительства США со штаб-квартирой в Калифорнии. Структура управления ICANN зиждется на коллективном Совете директоров из 18 человек, половина из которых назначается тремя аффилированными организациями, а вторая избирается на всемирных выборах среди ее членов в Интернете. Интересно, что ICANN до сих пор поддерживает домен SU, несмотря на то что СССР уже давно не существует, и отказывается запустить домен EU, который должен стать важным фактором консолидации стран Евросоюза. Структура крупнейших организаций, управляющих интернетом, не является постоянной и часто меняется. Необходимо знать, что в интернете фактически заложена возможность создания любых новых доменов, в т.ч. национальных, проблема - лишь в довольно большом количестве провайдеров (организаций, предоставляющих доступ в интернет), которые согласились бы поддерживать переадресацию на новые доменные зоны.

При реализации ряда сценариев мирового политического развития Интернет способен распасться на множество национальных и иных зон, вход и выход из которых будет контролироваться правительствами и иными субъектами мировой политики. Уже сегодня здесь функционирует несколько альтернативных зон, поддерживаемых крупными интернет-провайдерами. Кроме того, в Интернете есть много так называемых темных зон и сумеречных зон. «Темные зоны» невидимы для большинства пользователей; при этом их количество превышает 100 млн. адресов и составляет около 5% от общей их численности. В таких зонах расположены по преимуществу сайты военных ведомств США, использующих созданную в годы холодной войны адресную систему Milnet. «Сумеречные зоны» Интернета считаются заброшенными и используются хакерскими группами для организации DOS – атак[67].

2. Системы *серверов, кабелей* и *спутников*, через которые проходит интернет-трафик. На начало 2003 г. подавляющее большинство системообразующих серверов, поддерживающих DNS-адресацию (по некоторым данным, 9 из 13 самых крупных) находилось на территории США. По этим серверам проходит более половины глобального интернет-трафика, что дает Америке *потенциальную* возможность контроля над контентом Интернета. Ситуация во многом повторяется с кабельной системой. На территории России нет самостоятельной системы обмена трафиком, и отечественный трафик часто идет через зарубежные каналы. Российские сети передачи данных конкурируют или дублируют друг друга, что во многом связано с их ведомственной принадлежностью[68]. Мировая система спутникового обмена данными представлена системами «Iridium», «GlobalStar» и др. Большинство их были сконструированы, исходя из потребностей мобильной связи и передачи телесигнала, глобального позиционирования (GPS, ГЛОНАСС, Galileo), и не всегда приспособлены для передачи интернет-трафика, особенно в части потокового видео- и аудиосигнала.

3.Системы *поисковых механизмов* (англ. search engines) и *механизмов извлечения контента* (data mining). По оценкам аналитиков, сегодня крупнейшие поисковые системы (Google, Fast, Northern Light, Yahoo) совокупно индексируют не более 45% от общего количества страниц, размещенных в Интернете. Наиболее популярная и релевантная поисковая система (с механизмом ранжирования индексируемых страниц на основе

[67] Архитектура Интернета создавалась в условиях, когда внутри сети существовало доверие к действиям отдельных участников. В результате разросшийся Интернет несет на себе отпечаток "младенчества" и почти не содержит встроенные механизмы безопасности. Если участник сети (роутер) заявляет, что он владеет блоком адресного пространства, остальная часть Интернета верит ему на слово и адресует к нему весь соответствующий трафик. Значит, можно создать любой сетевой блок и запустить его в Интернет, придав анонимность любой атаке. "Сумеречные зоны", наряду с технологиями подмена авторства («спуфинг») кардинально меняют способы ведения войны в интернет-пространстве.

[68] Крупнейшие проекты кабельных систем передачи данных связаны с Газпромом, РАО ЕЭС и МПС России, что объясняется наличием в распоряжении последних развитой транспортной инфраструктуры.

предпочтений пользователей) - Google. Технология Google основана на учете мнения самих пользователей о веб-ресурсах. Существует мнение, что Google является прообразом «государства будущего», не нуждающегося в традиционных средствах подавления. Действительно, с поисковыми системами напрямую связан вопрос о механизмах и сути власти в интернете. Если представительства той или иной организации здесь не «обсчитаны» спайдерами поисковой системы, то для абсолютного большинства пользователей Интернета эта организация не существует. Такая ситуация создает в сети механизмы подавления и контроля отдельных акторов, следовательно, допускает возможность появления "онлайнового" варианта государства. В интернете действуют совершенно иные акторы, нежели в обычном мире, и совокупная мощь отдельной нации-государства, преломленная в киберпространстве, значительно уступает возможностям компании Google или общественного "онлайнового" сообщества, например, связанного с антиглобалистским движением. Исключение, подтверждающее правило, - США, которым доступен институциональный контроль над Интернетом, а самая уязвимая часть сети - инфраструктура. Существует множество мелких, по сравнению с гигантами типа Google, поисковых механизмов и средств индексации, в т.ч. представляющих закрытые корпоративные информационные системы и альтернативные пиринговые сообщества, типа Гнутеллы (Gnutella), Морфеус (Morpheus) или Казаа (Kazaa). Поисковые системы иногда используются для доступа к информации, которая блокируется национальными правительствами. Известна практика закрытия доступа к определенным сайтам правительством Китая, которое так борется с оппозицией коммунистическому режиму страны. Google кэширует (сохраняет копии) индексируемые страницы, что позволяет китайским оппозиционерам получать доступ к сайтам, которые в КНР запрещены. Блокировать подходы к самому Google значительно сложнее, ибо есть множество окольных путей доступа, в точ числе с использованием пиринговых технологий, разрабатываемых хакерскими группами (Pick-A-Booty).

В России в сфере поисковых систем с Google конкурирует компания Яндекс, постепенно перехватившая лидерство у компаний Rambler и Aport. Яндекс обсчитывает русскоязычные сайты, в т.ч. находящиеся на территории других стран, очерчивая потенциальные пределы виртуального «пространства Ru».

4. К системам *гейтов* и *периферийным структурам* относится то, для чего приоритетны иные способы коммуникации, например, передача голоса. Современные системы сотовой связи, начиная со стандарта GSM, позволяют получать и передавать данные, фактически становясь частью Интернета. В результате резко возрастает общее число его пользователей, а значит, и политические возможности. «Быстрые революции» и масштабные студенческие волнения в Иране, Филиппинах и Югославии были осуществлены во многом за счет использования синтеза Интернета и сотовых сетей. С помощью такого рода сетей становится организация т.н. «умных толп», хаотически, но при этом управляемо, появляющихся в любом месте, минимизируя возможности государства по предотвращению социальных выступлений. Фактически, происходит обратный перенос технологий интернета в традиционную социальную среду. Новые стандарты, от CDMA 2000 до I-mode, позволяют почти полностью интегрировать сотовые сети в структуру Интернета. Гейты, т.е. специальные сервисы, встраивают его в остальные традиционные средства коммуникации: телеграфную связь, почту, телефонию, телевидение, передачу информации о финансовых рынках и т.д., фактически замыкая на себя все виды опосредованной коммуникации человека. Развитие беспроводных сетей стандарта 802.11 и технологии VoiceOverIP в ближайшие 10-20 лет приведет к окончательной интеграции традиционных коммуникативных каналов и Интернета, создав глобальную информационную среду, удовлетворяющую критерию «любая информация в любом месте в любое время».

Эволюция интернет-технологий в современном мире совпадает с распространением других сетевых форм организации жизнедеятельности людей. Такое «ползучее разрастание» сетевых форм - безусловная угроза традиционному пониманию политики как совокупности

отношений по поводу власти. Последняя вписывается в культурные коды, с помощью которых люди определяют свои позиции на новом информационном поле. Решения на уровне институтов также принимаются посредством кодов, что приводит к разрыву с политической логикой традиционных институтов. Интенция парадоксальна – для обеспечения собственного существования, институты должны перестать быть самими собой, утратить свою статусную природу.

В деятельности политических институтов в Интернете выделяются три основные этапа, которые пересекаются, накладываются друг на друга или идут в обратной последовательности.

| Первый этап | Второй этап | Третий этап |
|---|---|---|
| Перенос или дублирование части своих функций в интернет-пространство | Создание параллельных или новых сетевых структур, обладающих самостоятельностью функций | Обратный перенос, конвертация, встраивание сетевых структур во взаимодействие реальных институтов |

Классификация акторов, используя терминологию Интернета, может выглядеть следующим образом.

**Акторы в политическом пространстве Интернета[69]**

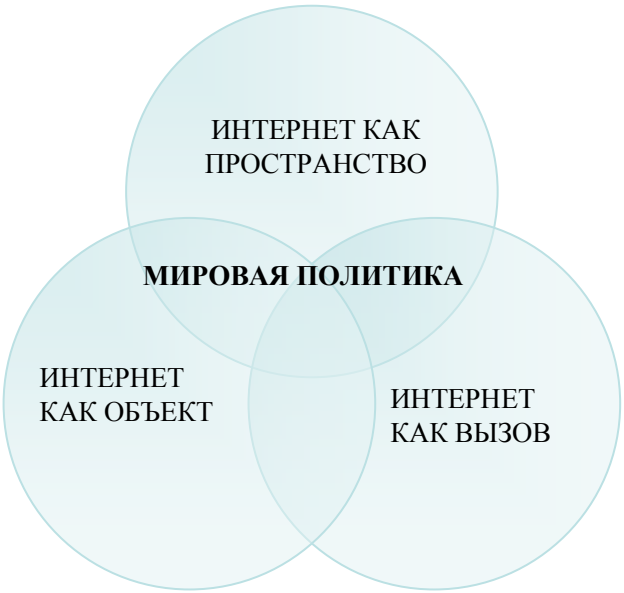

Существует различие между понятием актора в Интернете и традиционным субъектом. В интернете происходит размывание, смещение и «перехват» обычных функций актора. В большинстве случаев провести их четкое разграничение, используя традиционные методы политологии, невозможно. Так, в Интернете политическое действие, с одной стороны, персонализировано, ибо индивид получает массу возможностей, доступных в реальной жизни лишь целым институтам. С другой - оно может быть обезличено (как в случае с

[69] Под «онлайном» (англ. online) подразумевается виртуальная среда Интернета, существующая в реальном времени; «офлайн» (offline) означает традиционное взаимодействие в реальности.

применение сетевого компромата) или скрываться за бесконечным количеством nicknames (англ. личин) актора.

**Интернет как пространство, вызов и объект**

Применительно к мировой политике можно говорить о трех главных качествах, в которых выступает Интернет.




*Интернет как пространство мировой политики* подразумевает собственное использование в качестве своеобразного географического поля, отражающего традиционные политические институты.

В этом новом пространстве взаимодействуют традиционные и новые акторы, причем последние здесь доминируют, вытесняя государства и формальные международные организации на обочину интернет-политики. Ее ключевые вопросы, или, как их иногда называют, дихотомии Интернета:

- противостояние движения Open Source и разработчиков закрытого программного обеспечения, прежде всего компании Microsoft, - открытость и закрытость;
- противоречия мультимедийных компаний и их ассоциаций, в первую очередь RIIA (ассоциации звукозаписывающих компаний) и пользователей пиринговых систем (позволяющих скачивать любые, в т.ч. музыкальные, файлы, напрямую с компьютера другого пользователя), - платность и бесплатность;
- конфронтация государственных спецслужб и правозащитных организаций - безопасность и приватность;

- противопоставление практик законодательного и программного регулирования - законы и программы[70];

- антагонизм государственного суверенитета и сетевых организаций - запрет и свобода.

Сегодня основные вопросы интернет-политики, значимые для государств, - взаимоотношения с сетевыми организациями, борьба с киберпреступностью и информационные войны.

В первую половину 1990-х гг. большинство государств считали, что международные сетевые организации в конфликтных ситуациях представляют собой прямую угрозу национальной безопасности и пытались (в ряде случаев) действовать прямыми силовыми средствами, однако безуспешно. С середины 1990-х гг. все возникшие сколько-нибудь крупные социальные организации - это сети, построенные на основе Интернета. М. Кастельс выделяет три главные характеристики сетевых социальных движений: 1) все они структурированы вокруг разделяемых культурных ценностей, которые становятся основой для формирования организационной идентичности; 2) они заполняют собой нишу потерявших доверие граждан традиционных политических институтов, таких как партии, профсоюзы и формальные организации гражданского общества; 3) они стремятся к глобальности своего действия, так как именно всепланетарное распространение позволяет им эффективно действовать на локальном уровне.

В мировой политике стоит отметить примеры трех таких сетей: сети поддержки сапатистского движения, ставшей одной из основ современного антиглобалистского движения, сети Фалуньгунь, китайской религиозной организации с политическими целями, и сети движения за запрещение противопехотных мин. В первом случае целью сети было информационное содействие индейскому мексиканскому движению сапатистов во главе с субкомманданте Маркосом, а впоследствии, борьба с ТНК и мировыми финансовыми институтами. Во втором - лидер Фалуньгунь Ли Хонжи, проживая в Нью-Йорке, использовал Интернет как для доставки религиозных материалов своим последователям, так и для организации массовых манифестаций в конкретное время в определенном месте, что позволило ему бросить вызов политическому режиму в Китае (по сути, впервые со времени событий на площади Тяньаньмэнь). В третьем, менее типичном случае, объединенным в сеть организациям, созданным под конкретный проект – законодательное запрещение применение противопехотных мин на международном уровне – удалось организовать эффективную лоббистскую кампанию одновременно на национальных и международном уровнях, объединяя в коалиции разнородные гражданские организации, и преодолеть сопротивление США, которые противодействовали принятию данного законопроекта.

Во всех случаях нациям-государствам не удалось организовать эффективное противодействие, причем ни в онлайне, ни в офлайне. Так, даже полная мобилизация итальянской полиции, закрытие границ и приостановление действия шенгенских соглашений на территории страны не предотвратили проникновение на собрание «большой восьмерки» в Геную более 100 тыс. антиглобалистов, координировавших свои действия через Интернет. Итальянское правительство фактически признало свою неспособность справиться с их выступлениями, призвав устами С. Берлускони перенести следующую межгосударственную встречу по продовольственным программам из Рима в одно из африканских государств. Такие формы акций не могут быть осознаны в рамках традиционных концепций международных отношений. Недаром в попытках анализа деятельности антиглобалистов обычно звучит идея «мирового заговора», неких теневых структур, стоящих за манифестантами. Гораздо легче понять и принять последнюю идею, чем смириться с тем, что

[70] Переходное состояние между законами и программами принадлежит к области "soft law" – выработанных на основе перекрестного консенсуса правил. Такой подход гораздо гибче, но требует более сложного согласования процесса изменения уже имеющихся правил, так как количество участников растет по экспоненте и даже при горизонтальной коммуникации необходимы институты согласования и принуждения, хотя бы в форме общественного порицания участников сети, не соблюдающих правила, и их последующего осуждения.

Интернет стал не только новым техническим средством, но и перешел в контрнаступление, меняя по своему образу и подобию окружающую социальную действительность[71]. Кроме того, интернет-сопротивление легко абсорбирует независимые, в т.ч. террористические, формы протеста[72].

Борьба с киберпреступностью - другой важнейший фактор, влияющий на политику государств в Интернете. Преступность, как и другие феномены современного миры, преломляется здесь самым неожиданым образом. Традиционные криминальные сообщества используют возможности Интернета для координации действий. Часто интернет-форумы работают как своеобразные биржи, где можно купить наркотики, нанять киллера или легализовать средства, полученные нелегально. Типичный пример такой биржи – форум на сайте www.bratok.com. Далее, Интернет привел к появлению новых форм преступности, среди которых наиболее масштабные - сетевая порнография и кардинг (преступления, связанные со взломом, подделкой и использованием кредитных карточек). Вокруг этих явлений, крепко, хотя и не напрямую обусловленных хакерством, очень быстро сложились профессиональные криминальные сообщества с характерным сленгом и способами коммуникации. Они почти полностью живут в информационном обществе, так как Интернет является для них единственным источником и средой существования. Онлайновая преступность широко использует технические новшества и возможности Интернета, неактуальные для большей части пользователей[73]. Усилия государств в борьбе с такими сообществами резко возрастают при межгосударственной координации и создании «профильных» сетевых правоохранительных органов, что наглядно демонстрируют случаи успеха в борьбе с детской порнографией в Интернете. Подобные структуры существуют при Интерполе и ряде других организаций. С другой стороны, нескоординированные действия отдельных государств в борьбе с киберпреступностью приводят к возникновению сложных дипломатических коллизий, разрешение которых не может происходить ни на национальном уровне, ни на уровне двусторонних договоров. Примером такой коллизии может служить дело арестованных в 2000 году в США челябинских хакеров Горшкова и Иванова. В ходе расследования дела ФБР взломало сервер, физически расположенный на территории России, не получив соответствующего разрешения от российских правоохранительных органов. В ходе судебного слушания судья признал улики, добытые подобным образом, законными, заявив, что «преступность не имеет границ». Таким образом, учитывая прецедентный характер американского правосудия, ФБР и другие спецслужбы получили право действовать в киберпространстве, не обращая внимание на национальную принадлежность того или иного домена. Государственный суверенитет, таким образом, не распространяется автоматически на киберпространство. Эта проблема остается на сегодняшний день неразрешенной, процесс законодательной борьбы с киберпреступностью крайне сложен. Тем не менее, определенные шаги в этом направлении предпринимаются.

В декабре 1997 г. на встрече министров внутренних дел и юстиции государств "восьмерки" в США был подписан документ «Принципы и план действий по борьбе с высокотехнологическими преступлениям». В мае 2002 г. на встрече ее представителей в Париже была достигнута договоренность о принятии странами «восьмерки» аналогичных

---

[71] Влияние Интернета на действительность часто недооценивается. Можно говорить об изменениях в структуре общественного сознания, связанных с эрозией морали (распространение порнографии и личины, права (споры за «доменные имена», «вирусные» лицензии, электронная подпись, копирайт), политики (пропаганда, создание компромата), международных отношений (отсутствие в сети государственного суверенитета).

[72] Показательны во многом параллельные примеры субкоммандante Маркоса, вышедшего со своей «геометрической» антиглобалистской программой из обычного мексиканского штата через Интернет на уровень мировой политики, и М. Удугова, создателя сайта чеченских сепаратистов «Кавказ», эффективно противодействовавшиго государственной российской пропаганде во время первой чеченской кампании. Не менее эффективна сегодня и информационная кампания «Аль-Каиды» в арабском мире.

[73] Онлайновое сообщество российских веб-мастеров порноиндустрии широко использует феномен «GoogleDance», время переиндексации контента в поисковой системе, когда есть шанс продвинуть свой сайт в первую сотню (десятку, двадцатку) результатов запроса пользователя, от чего напрямую зависит их заработок.

законов по борьбе с киберпреступностью на национальном уровне. В ноябре 2001 г. на конференции в Будапеште представителями 30 стран (в т.ч. 26 государств-членов Совета Европы, а также США, Канады, Японии и ЮАР) была подписана Конвенция по киберпреступности (англ. Convention on Cybercrime). Согласно документу, должен быть создан специальный межгосударственный орган, работающий в круглосуточном режиме (т.е. в режиме интернет-времени) и имеющий полномочия по удалению материалов вне зависимости от физического местонахождения интернет-ресурса. Согласовывались национальные законодательства, режим розыскных мероприятий, также предусматривалась разработка системы наказания преступников. Фактически, документ подразумевал создание международной киберполиции с самыми широкими правами. Ратификация договора затянулась, и на данный момент он в действие не вступил. В целом растущие масштабы киберпреступности - мощный довод в пользу создания защищенных и подконтрольных государству участков Интернета, а также внедрения государственных технологий идентификации пользователей им.

Распространение Интернета, спустя 30 лет после его создания, теперь существенно влияет на сферу, где он был образован. Принципы сетевой организации, пиринговое взаимодействие, абсолютизация роли информации в инфраструктуре государства – все эти факторы привели к началу настоящей революции в военных аспектах международных отношений и мировой политики. В соответствующих концепциях государств появляется понятие информационной войны, различные определения информационного оружия. Единой, или сколько-нибудь общеупотребительной, классификации информационного оружия не существует. По сути дела, любое из них может с каким-то основанием названо информационным. Важно понимать, что объектом воздействия в информационной войне, и вообще в войне нового типа, является не только военная инфраструктура противника, но и его общая инфраструктура управления страной, ее население. Чем более развита страна, тем уязвимее ее инфраструктура. Угрозы для нее способны исходить отовсюду, в т.ч. от индивидов, террористических группировок и т.д. Если военные системы управления обычно довольно хорошо защищены и не имеют гейтов, связывающих их с Интернетом, то системы управления движением, энергетические и коммунальные структуры очевидно подвержены таким угрозам. Так, Китай в 2001 г. признал невозможность достижения в обозримой перспективе паритета с США в области обычных вооружений и поставил на развитие информационного оружия, в т.ч. с использованием китайской диаспоры в других странах, что позволяет ему де-факто «окружить» потенциального противника и нанести ему удары изнутри. Есть данные о том, что во время потенциального конфликта между США и КНР китайские хакеры (с применением вирусов типа «троянский конь») получили бы доступ к энергетическим системам в Калифорнии. Во время энергетического кризиса на северо-западе США одной из причин кризиса называли воздействие вируса Sobig. Документально данное воздействие не зафиксировано, но в ходе борьбы с вирусом Sobig произошел весьма показательный инцидент. Для борьбы с вирусом неизвестным доброжелателем был написан другой вирус Wellchia, с аналогичными принципами распространения. Новый вирус находил Sobig на компьютере пользоватлея и уничтожал его, после чего самоуничтожался сам. На практике борьба между вирусами привела к перегрузке систем в системах управления авиадвижением в Канаде и сбоях в полетах самолетов. Учитывая, что в той же Канаде каналы VPN (Virual Private Network) используются для управления атомными электростанциями, угроза неконтролируемой вирусной эпидемии становится крайне вероятной. Тотальный выход из строя энергетической и/или коммуникационной системы страны, между тем, вполне может быть сравним по масштабу своего воздействия с ограниченным применением ядерного оружия. В информационной войне есть и аналогии массового применения ядерного оружия. Так, существуют вирусы, выводящие из строя не все компьютеры, а только те, на которых не установлена определенная кодировка, например, Cyrillic. При массированном использовании вируса такого рода, «посаженного» на червя нового типа, против которого не существует «заплаток» антивирусных компаний, будут

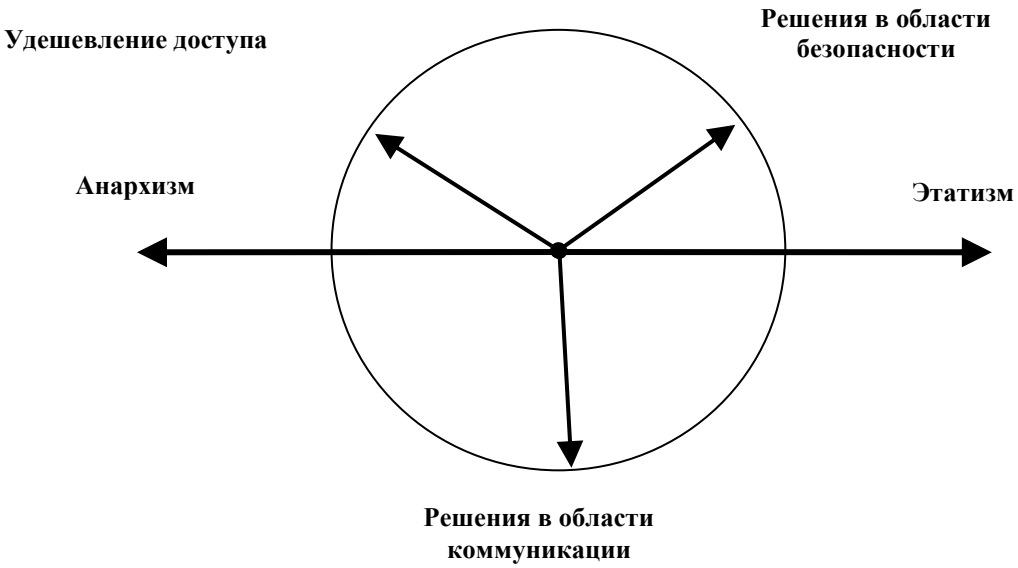
выведены из строя *все подключенные* к Интернету компьютеры, кроме российских. Противодействием попыткам такого рода стало бы применение средств сильного шифрования, основанного на 128-битных и выше ключах, которые доступны коммерчески и не имеют известных средств взлома. Однако здесь потенциальные интересы национальной безопасности входят в противоречие с желанием современных государств контролировать своих граждан, что приводит к запретам на повсеместное употребление сильного крипто.

Изменяется и структура вооруженных сил, как и само понятие вооружения. Появляется новая тактика «swarming» - "роение", при котором на поле боя (как виртуальном, так и реальном) действуют мобильные автономные группы, обладающие горизонтальными средствами коммуникациями и правом инициативы в рамках предложенной стратегии. При этом на удаленном командном пункте присутствует вся картина боевых действий. «Рой» скапливается в местах нанесения удара и моментально рассыпается, не теряя общего управления. В США при разработке новой тактики используется опыт маоистом, приемы городской герильи, опыты сапатистов и чеченских сепаратистов. Так, в 2000 г. в Америке были проведены учения морских пехотинцев "Chechen Swarming", в ходе которых была опробован система C4ISR (command, control, communications, computers, intelligence, surveillance, reconnaissance), основанная на тактике "роения"[74].

Военные аналитики, например, в этой стране считают наступившие изменения значительными настолько, чтобы вновь противопоставить концепцию Realpolitik концепции Noopolitik – принципу действия в глобальной информационной среде, ноосфере, включающей в себя не только Интернет, но и все медийные средства коммуникации. Realpolitik не исчезает в новой среде, мощь государства остается значимым фактором международных отношенИй, но в мировой политике отныне господствует логика открытых сетевых систем, в т.ч. государственных. Развитие Интернета и глобальных политических систем нового типа, построенных на сетевых принципах, вносит ряд дополнительных аргументов в копилку представителей постмодернистских теорий международных отношений. Постмодернизм вполне адекватно описывает современные и политическую реальность, и политическую виртуальность Интернета. Принимая взгляд на Интернет в состоянии "предгосударства" как модели завтрашнего общественного устройства, мы вынуждены констатировать актуальность разработок постмодернизма как для анализа процессов внутри сети, так и для рассмотрения современных международных отношений и мировой политики. Речь идет о работающих в Интернете и политических сетях концептах ризомы Гваттари, смешения и симулякра Бодрийяра, спектакля Барта, паратемы Фуко, политического поля Бурдьё. Фактически постмодернизм предоставляет нам механизмы анализа новой действительности.

Интернет способен влиять на различные политические процессы в прямо противоположном направлении. В зависимости от вектора применения его возможности могут использоваться для повышения уровня участия граждан в политике или для тотального контроля государства над своим населением. Интересно, что три основные тенденции, характеризующие развитие Интернета в начале XXI в. - *удешевление доступа к нему*, что делает его потенциально приемлемым для абсолютного большинства жителей индустриальных стран; *решения в области коммуникации,* создающие реальную глобальную информационную среду; *постановления в сфере безопасности*, которые позволяют контролировать все акции в сети, - придают ему возможность любого социального конструирования на основе интернет-технологий: от абсолютно анархического общества до тоталитарного государства, описанного Дж. Оруэллом в романе «1984».

[74] См.: Arquilla J., Ronfeldt D. *Swarming and the Future of Conflict*. Santa Monica, CA: Rand National Defense Research Institute, 2000.




В пространстве Интернета проявляются и новые факторы влияния на мировую политику и положение государств на планете. Их роль сегодня скорее минимальна, но она постоянно возрастает, и мы можем прогнозировать совершенно новые области политических отношений в сети. Речь идет о хакерских сообществах, виртуальных социальных и квазигосударственных образованиях, компьютерных агентах, вирусах и игровых вселенных. Хакерские сообщества уже сейчас заметны в отдельных событиях мировой политики – от участия в информационных войнах во время отдельных конфликтов (США – Китай, Палестина – Израиль, США – Ирак и т.д.) до антиглобалистских акций (кража и распространение секретной информации во время Давосского форума), разработки специальных программных продуктов, позволяющих пользователю Интернета обходить любой государственный контроль (пиринговый клиент Peek-A-Booty). В нем ныне существует множество виртуальных образований: от интернет-партий (www.internetparty.org) до псевдогосударств (- www.sealandgov.com) и своеобразных отражений реальных стран (www.respublika.ru В. Третьякова). Компьютерные агенты получат в Интернете широкое распространение с его эволюцией в сторону Semantic Web, т.е. сети с элементами искусственного интеллекта. Типичный пример такого агента – компьютерный бот (робот), созданный для выполнения определенного набора задач (например, создания сообщества, распространения (дез)информации, блокирования сайтов и т.д.). С развитием таких агентов тесно связан рост вирусов. По прогнозам, к 2012 г. каждое второе электронное сообщение будет заражено вирусом. Последние также получают элементы искусственного интеллекта, способность к неконтролируемому размножению путем клонирования, спаривания, следовательно, - к мутированию и эволюции. Вирусы в определенный момент могут привести к отказу от разрастания Интернета в его сегодняшнем виде и переходу к иной архитектуре сети с преимущественно вертикальной иерархией. Еще одной областью политического в Интернете могут стать онлайновые игровые миры, где стирается грань между реальностью и виртуальностью. Игровые предметы в таких мирах покупаются и продаются за реальные деньги, игра может служить для реального заработка; преступления в виртуальном мире начинают преследоваться по реальным законам, действия проходят частично в реальности. Уже сегодня экономика онлайновых миров оценивается в десятки миллиардов долларов – сегодня это самая быстрорастущее хозяйство на Земле, а три года назад его просто не существовало. Игровые миры, между тем, являются мощным средством социального конструирования, включая создание реальной идентичности *нетизена* – гражданина Интернета. По силе своего воздействия такие миры превосходят книги, радио и телевидение. Прообразы подобных миров сделаны корпорацией Sony (www.everquest.com) и уже используются, например, для продвижения бренда внутри сообщества. Еще одна сфера

игровых миров - тренинги в вооруженных силах. В США тактика ближнего боя (в т.ч. пехотного, танкового и авиационного) на уровне отдельных подразделений полностью моделируется на симуляторах реальности, заменяя и дополняя дорогие маневры. Подобные модели начинают использоваться армиями других стран. Тактика городской герильи в Москве, к примеру, легко моделируется с помощью общедоступной игры на мобильных телефонах по типу Botfighters компании Мегафон.

*Интернет как вызов мировой политике* в узком смысле слова является технологией, т.е. тем, что, наравне с законами, политическими и экономическими институтами, обычаями и культурными системами, является социальной структурой, которая формирует жизнь общества и влияет на эволюцию человека. Интернет, *воздействуя* на все выше перечисленные *социальные структуры* и будучи принципиально новой из них, представляет собой *вызов* традиционным. Интенция парадоксальна – для своего выживания институты должны видоизмениться, утратив часть своей статусной структуры. Подавляющее большинство нововведений в информационных, социальных и биологических технологиях тесно связаны с Интернетом и обязаны ему своим существованием. Это объясняется тем, что сегодня именно здесь скапливается *все новое знание мира*. Традиционные модели создания и распространения научных знаний остаются в прошлом и абсорбируются Интернетом. Основной формой коллектива, создающего знание, становится распределенная сетевая междисциплинарная группа, работающая над проектом либо их группой. Правительства как субъекты не способны вырабатывать новшества в Интернете, они лишь в состоянии создавать климат, препятствующий либо помогающий появлению таких нововведений. Сверх того, изобретения используют не государства, а общественные организации, отдельные личности или корпорации. Государства как наиболее инертные институты сейчас только реагируют на социальные, правовые либо политические последствия подобных новшеств.

Так, выбор культуры потребления, в т.ч. связанный с информационным миром, ныне почти полностью ушел из сферы влияния наций-государств и отдан корпорациям. Применение моделей Microsoft в школьном образовании ведет к появлению поколения пользователей систем, целиком зависящих от удаленного управления. Выбор Linux заставляет сложиться генерацию разработчиков систем, способных создавать вокруг себя работающие модели кооперации. В России для системы начального, среднего и высшего образования выбор делается в пользу Microsoft, а в Китае – за Linux. В общем смысле выбор формулируется так: либо политики определяют, какие технологии будут использоваться для развития общества, либо технологические корпорации внедряют через рынок принципы новых технологий, которые через поколение обусловят выбор вектора политического развития.

Однако в последние пять лет большинство стран воспринимают и реагируют на вызов Интернета на государственном уровне. Можно выделить следующие типы реакций на появление глобальной информационной среды: отторжение, принятие, принятие с ограничениями, использование, ставка на развитие. Основная задача, стоящая перед развитыми нациями-государствами, которые активно участвуют в мировой политической системе и делают ставку на развитие Интернета, - адекватный переход на интернет-качество государственных и общественных структур, конвергенция государства и общества на основе информационных технологий. Вектор однозначен, он вербализируется интеллектуалами, продвигается бизнесом и верифицирован правительствами[75]. В 2000 г. на встрече «восьмерки» была принята Окинавская хартия, декларировавшая приверженность ведущих

[75] Народившийся "класс" (пока в кавычках) интернет-пользователей требует нововведений и приближения стандартов офлайна к возможностям онлайна. Этот "класс" - основная движущая сила, предположительно, нового революционного процесса, а так как его представители априори являются богаче, мобильнее и влиятельнее тех, кто работает в офлайне, то они с большим успехом влияют на процессы принятия решений, касающиеся создания интернет-государств и т.д. Чем больше влияния, тем больше людей включаются в их "класс" и становятся носителем его идеологии, тем больше их совокупное воздействие на мир.

стран мира созданию глобального информационного общества. На встрече была образована группа DOT-Force (т.е. по возможностям информационных технологий), которая призвана объединить усилия стран по формированию единого подхода к решению ключевых проблем на пути сотворения глобального информационного общества, прежде всего по вопросам "цифрового неравенства" (англ. digital divide) и формирования так называемых электронных правительств (e-governments).

Развитие технологий информационного общества - обязательно для стран, намеренных активно участвовать в международных экономических и политических отношениях. Россия декларирует свою приверженность данному пути, но сопротивление традиционных институтов внутри страны ставит под сомнение возможность полноценного включения в международные институты нового поколения вроде ВТО.

Государства, выигравшие информационную гонку, получают три типа бонусов:

- *непосредственные* за счет порядкового увеличения эффективности существующих функций;
- *тактические* из-за получения новых функциональных возможностей, таких как диаспоральное управление на глобальном уровне;
- *стратегические* в силу способности устанавливать *свои* правила игры на пока возникающей территории – информационном поле. Ситуацию усложняет появление новых типов игроков: транснациональные корпорации и социальные сетевые организации тоже претендуют на собственную долю суверенитета и господства в информационном мире.

Информационная гонка, или Internet race, современных государств, может измеряться и оцениваться десятками разных способов, включая анализ количественных и качественных данных. Существуют и интегрированные рейтинги, оценивающие «степень готовности» различных государств к информационному обществу. Network Readiness Index, подготовленный в 2002 г. Center for International Development (CID) Гарвардского университета, ставит Россию на 61 место из 75 стран, рассматривавшихся в рейтинге. Первые три места занимают США, Исландия и Финляндия. Общая оценка складывается из совокупности таких параметров, как развитость: информационной инфраструктуры, национальной политики в области информационно-коммуникативных технологий, экономического климата, социального капитала, онлайнового обучения, электронной коммерции и государственного управления.

Агрегированным результатом информационного развития становится создание систем «электронных правительств». На сегодня удачных комплексных решений по формированию «e-governments» не существует. Очевидно, что имеющаяся инфраструктура с обособленными каналами передачи данных не позволит реализовать модели государственного устройства нового типа на сколько-нибудь обширной территории. Показательно, что государство, наиболее приблизившееся к стандарту "электронного правительства" – Сингапур, – обладает весьма ограниченной территорией и авторитарным режимом правления.

Основным инструментом перехода к информационному обществу обычно выступают специализированные государственные программы, аккумулирующие возможности государства, общества и бизнеса. В целом аналогичные программы приняты большинством европейских стран, рядом государств Центральной и Южной Америки и Юго-Восточной Азии. Ключевые элементы таких программ - обеспечение дешевого и всеобщего доступа в Интернет, развитие "электронных правительств", онлайнового бизнеса и обучения. В нашей стране с 2001 г. осуществляется программа «Электронная Россия».

*Интернет как объект*, отдельное пространство, остается сегодня на периферии мировой политики. Вопросам его регулирования и развития в качестве объекта уделяется непропорционально мало внимания. Такой парадокс объясняется рядом причин:

- глобальностью Интернета и его "связностью": любое регулирование на национальном уровне без учета глобального характера Интернета приведет лишь к исключению страны из мирового информационного обмена, ценность этого пространства состоит именно в возможности соединить гиперссылкой два любых места;

- историческими особенностями регулирования Интернета, ролью культурного фактора и особенностями личности людей, создавших и развивавших его в 1990-е гг.;
- общей сложностью и постоянной эволюцией Интернета, когда скорость протекания здесь внутренних процессов на много порядков превосходит возможности оперативного регулирования со стороны государства;
- принципиальными противоречиями между понятиями суверенитета и личности в Интернете и в мире.

В 1990-е гг. Интернет остается фактически вне сферы правового и политического регулирования внутри наций-государств. В мировой политике складывается ситуация, когда почти все страны заинтересованы в развитии интернет-пространства, однако при этом хотели бы распространить свою юрисдикцию на его территорию. Правовые отношения в Интернете затрагивают проблемы: юрисдикции отношений между пользователями; ответственности контент-провайдеров; саморегулирования стандартов и протоколов. Общемировая практика правового регулирования Интернета сводится на сегодня к ряду противоречивых судебных решений, определяющих государственную юрисдикцию. Это связано с тем, что для него отсутствуют так называемые коллизионные нормы (например, lex patrie – закон гражданства, lex loci actus – закон места совершения сделки и т.д.). Так, американский суд в 2001 г. постановил: действия, предпринятые спецслужбами США по взлому сервера, расположенного на территории Челябинской области, в рамках уголовного дела против двух отечественных хакеров Иванова и Горшкова - законны, несмотря на то что Россия не давала согласия на подобные меры. Пути урегулирования статуса Интернета расположены в сферах заключения многосторонних соглашений, принятия международных договоров и постепенной унификации национальных законодательств по данному вопросу. Пока единственный серьезный шаг - европейская Конвенция о киберпреступности, подписанная 30 государствами, но на сегодня ратифицированная только Албанией. Такому процессу препятствуют прежде всего неодинаковые политические режимы стран субконтинента и, соответственно, различия в подходах к регулированию Интернета. Режим контроля над провайдерами контента и доступа в него - в диапазоне от практически тотального (Саудовская Аравия, Северная Корея, Ирак, Ливия) до ограниченного вмешательства в отношения внутри сети и предоставления иммунитета провайдеру за действия своих пользователей (США).

Террористические акты 11 сентября 2001 г. против городов США усилили вмешательство государств в упорядочение интернета, хотя и не привели к замене существующей на сегодня практике его саморегулирования. Предположительно, что в ближайшие пять-семь лет давление государств приведет к изменению в структуре Интернета. Кроме того, следует ожидать, что мировая политическая система (или глобальное общественное устройство) подвергнется не меньшим изменениям. Роль Интернета в них может оказаться решающей.

**Список литературы:**

1. The Digital Dilemma: Intellectual Property in the Information Age. Copyright 2000, the National Academy Press.
http://books.nap.edu/html/digital_dilemma/
2. Howard Rheingold's The Virtual Community.
http://www.rheingold.com/vc/book/
3. Donald Gutstein E.Con: How the Internet Undermines Democracy.
http://www.wr.com.au/democracy/
4. Ahtisaari, M. "Communications and the Global Conditions for World Peace". Intermedia. 1994.
5. Barlow, J.P. Old Wine in New Bottles.
http://www.eff.org/homes/barlow.html
6. LANGUAGE AND DIPLOMACY Edited by Jovan Kurbalija and Hannah Slavik. Malta, 2001.
http://diplo.diplomacy.edu/Books/language_and_diplomacy/default.htm
7. The Internet Guide for Diplomats Edited by Jovan Kurbalija and Stefano Baldi. Malta, 2000.
http://diplo.diplomacy.edu/
8. Knowledge and Diplomacy. Edited by Jovan Kurbalija. Malta, 1999.

http://diplo.diplomacy.edu/Publishing/knowledge/
9. Comparing Diplomatic Services: Structures, Networks and Resources of the Ministries of Foreign Affairs of EU and G8 Member States. Andrea Cascone. Malta, 2001.
10. Virtual diplomacy / I N T E R N E Tional Politics Year 0, number 3 - June 2001.
http://www.diplomaticnet.com/uk/index.php
11. Sites related to virtual diplomacy/ I N T E R N E Tional Politics Year 0, number 3 - June 2001.
http://www.diplomaticnet.com/uk/index.php
12. Sovereignity and Internet / I N T E R N E Tional Politics Year 0, number 2 - June 2001.
http://www.diplomaticnet.com/uk/index.php
13. States in Internet / I N T E R N E Tional Politics Year 0, number 1 - June 2001.
http://www.diplomaticnet.com/uk/index.php
14. Joseph S. Nye, Jr. Governance in the Information Age. Harvard, 2000.
http://www.ksg.harvard.edu/iip/governance/GlobCommDHVMS.PDF
15. Jane Fountain The Virtual State? Toward a Theory of Federal Bureaucracy in the 21st Century
http://www.ksg.harvard.edu/visions/fountain.htm
16. Deborah Hurley and Viktor Mayer-Schönberger, Information Policy and Governance, in *Governance in a Globalizing World*, ed. Joseph S. Nye, 2000.
http://www.ksg.harvard.edu/iip/governance/InfoPolicyDHVMS.PDF
17. Gernot Brodnig Virtual Diplomacy Project
http://ksghome.harvard.edu/~.vmayerschoenberger.academic.ksg
18. Jean Camp An Introduction to Internet Protocol and Domain Names
http://www.ksg.harvard.edu/people/jcamp/ICANNIP.pdf
19. Pippa Norris Democratic Phoenix: Political Activism Worldwide (New York: Cambridge University Press, 2002)
http://ksghome.harvard.edu/~.pnorris.shorenstein.ksg/everyvoice.htm
20. Pippa Norris. *A Virtuous Circle: Political Communications in Post-Industrial Democracies.*
http://www.ksg.harvard.edu/people/pnorris/mediated.htm
21. Yoshihara, Toshi "Chinese Information Warfare: A Phantom Menace or Emerging Threat?," in *Guest Presentations, Spring 2001.*
http://pirp.harvard.edu/pubs_pdf/yoshiha\\yoshiha-i01-3.pdf
22. Witte, Jan Martin, Wolfgang H. Reinicke and Thorsten Benner. "Beyond Multilateralism: Global Public Policy Networks." International Politics and Society 2/2000.
23. Вольфганг Х. Райнике, Торстен Беннер. Политика в глобальной сети.
http://www.deutschebotschaft-moskau.ru/ru/library/internationale-politik/1999-08/article05.html
24. "Critical Choices: The United Nations, Networks, and the Future of Global Governance".
http://www.globalpublicpolicy.net/Critical%20Choices%20Final.pdf
25. Кастельс М. Информационная эпоха. М., 1999.
http://www.buk.irk.ru/library/index.htm
26. Шадрин А. Информационное общество и политические процессы.
http://www.isn.ru/index122.shtml
27. Луман Н. Глобализация мирового сообщества: как следует системно понимать современное общество. - *Социология на пороге XXI века: новые направления исследований*. М. 1998.
28. Д.Песков. Интернет как политический институт в России http://www.isn.ru/public/project.doc
29. И.Пашкевич. Электронное правительство как показатель "зрелости" государственной власти http://www.e-government.ru/pub/e-government/985424172.html
30. Окинавская Хартия Глобального Информационного Общества (G8)
http://www.iis.ru/events/okinawa/charter.ru.html
31. Декларация о европейской политике в области новых информационных технологий http://www.telecom-media.com.ua/dosie/other/023.shtml
32. Новая постидустриальная волна на Западе (Сборник работ. Под редакцией В.Л.Иноземцева)
http://www.postindustrial.ru/titles5.shtml?book=7
33. Херфрид Мюнклер. Терроризм как стратегия коммуникации.
http://www.deutschebotschaft-moskau.ru/ru/library/internationale-politik/2001-12/article03.html

**Источник:** http://www.isn.ru/info/seminar-doc/peskov.doc (14.10.2011)

## ОКИНАВСКАЯ ХАРТИЯ ГЛОБАЛЬНОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА

*Принята 22 июля 2000 года лидерами стран G8, Окинава*

1. Информационно-коммуникационные технологии (ИТ) являются одним из наиболее важных факторов, влияющих на формирование общества двадцать первого века. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. ИТ быстро становятся жизненно важным стимулом развития мировой экономики. Они также дают возможность частным лицам, фирмам и сообществам, занимающимся предпринимательской деятельностью, более эффективно и творчески решать экономические и социальные проблемы. Перед всеми нами открываются огромные возможности.

2. Суть стимулируемой ИТ экономической и социальной трансформации заключается в ее способности содействовать людям и обществу в использовании знаний и идей. Информационное общество, как мы его представляем, позволяет людям шире использовать свой потенциал и реализовывать свои устремления. Для этого мы должны сделать так, чтобы ИТ служили достижению взаимодополняющих целей обеспечения устойчивого экономического роста, повышения общественного благосостояния, стимулирования социального согласия и полной реализации их потенциала в области укрепления демократии, транспарентного и ответственного управления, прав человека, развития культурного многообразия и укрепления международного мира и стабильности. Достижение этих целей и решение возникающих проблем потребует разработки эффективных национальных и международных стратегий.

3. Стремясь к достижению этих целей мы вновь подтверждаем нашу приверженность принципу участия в этом процессе: все люди повсеместно, без исключения должны иметь возможность пользоваться преимуществами глобального информационного общества. Устойчивость глобального информационного общества основывается на стимулирующих развитие человека демократических ценностях, таких как свободный обмен информацией и знаниями, взаимная терпимость и уважение к особенностям других людей.

4. Мы будем осуществлять руководство в продвижении усилий правительств по укреплению соответствующей политики и нормативной базы, стимулирующих конкуренцию и новаторство, обеспечение экономической и финансовой стабильности, содействующих сотрудничеству по оптимизации глобальных сетей, борьбе со злоупотреблениями, которые подрывают целостность сети, по сокращению разрыва в цифровых технологиях, инвестированию в людей и обеспечению глобального доступа и участия в этом процессе.

5. Настоящая Хартия является прежде всего призывом ко всем как в государственном, так и в частном секторах, ликвидировать международный разрыв в области информации и знаний. Солидная основа политики и действий в сфере ИТ может изменить методы нашего взаимодействия по продвижению социального и экономического прогресса во всем мире. Эффективное партнерство среди участников, включая совместное политическое сотрудничество, также является ключевым элементом рационального развития информационного общества.

### Использование возможностей цифровых технологий

6. Потенциальные преимущества ИТ, стимулирующие конкуренцию, способствующие расширению производства, создающие и поддерживающие экономический рост и занятость,

имеют значительные перспективы. Наша 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 важно строить работу на следующих ключевых направлениях:

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 новых информационных технологий;

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 ИТ во многих секторах нашей экономики;

активное использование ИТ в государственном секторе и содействие предоставлению в режиме реального времени услуг, необходимых для повышения уровня доступности власти для всех граждан.

7. Частный сектор играет жизненно важную роль в разработке информационных и коммуникационных сетей в информационном обществе. Однако задача создания предсказуемой, транспарентной и недискриминационной политики и нормативной базы, необходимой для информационного общества, лежит на правительствах. Нам необходимо позаботиться о том, чтобы правила и процедуры, имеющие отношение к ИТ, соответствовали коренным изменениям в экономических сделках с учетом принципов эффективного партнерства между государственным и частным сектором, а также транспарентности и технологической нейтральности. Такие правила должны быть предсказуемыми и способствовать укреплению делового и потребительского доверия. В целях максимизации социальной и экономической выгоды информационного общества мы согласны со следующими основными принципами и подходами и рекомендуем их другим:

продолжение содействия развития конкуренции и открытию рынков для информационной технологии и телекоммуникационной продукции и услуг, включая недискриминационное и основанное на затратах подключение к основным телекоммуникациям;

защита прав интеллектуальной собственности на информационные технологии имеет важное значение для продвижения нововведений, связанных с ИТ, развития конкуренции и широкого внедрения новых технологий; мы приветствуем совместную работу представителей органов власти по защите интеллектуальной собственности и поручаем нашим экспертам обсудить дальнейшие направления работы в этой сфере;

важно также вновь подтвердить обязательство правительств использовать только лицензированное программное обеспечение;

ряд услуг, включая телекоммуникации, транспорт, доставку посылок, имеют важное значение для информационного общества и экономики; повышение их эффективности и конкурентоспособности позволит расширить преимущества информационного общества; таможенные и экспедиторские процедуры также важны для развития информационных структур;

развитие трансграничной электронной торговли путем содействия дальнейшей либерализации, улучшения сетей и соответствующих услуг и процедур в контексте жестких рамок Всемирной торговой организации (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 недискриминацию, равноправие, упрощенность и прочие ключевые 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;

продвижение 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 подтверждение 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 это свободный поток информации, а также;

дальнейшее развитие и эффективное функционирование электронной идентификации, электронной подписи, криптографии и других средств обеспечения безопасности и достоверности операций.

8. Усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности киберпространства. Мы должны обеспечить осуществление эффективных мер - как это указано в Руководящих принципах по безопасности информационных систем ОЭСР - в борьбе с преступностью в компьютерной сфере. Будет расширено сотрудничество стран "Группы восьми" в рамках Лионской группы по транснациональной организованной преступности. Мы будем и далее содействовать установлению диалога с представителями промышленности, развивая, таким образом, успех, достигнутый на недавно прошедшей Парижской конференции "Группы восьми" "Диалог между правительством и промышленностью о безопасности и доверии в киберпространстве". Необходимо также найти эффективные политические решения актуальных проблем, как, например, попытки несанкционированного доступа и компьютерные вирусы. Мы будем и далее привлекать представителей промышленности и других посредников для защиты важных информационных инфраструктур.

**Преодоление электронно-цифрового разрыва**

9. Вопрос о преодолении электронно-цифрового разрыва внутри государств и между ними занял важное место в наших национальных дискуссиях. Каждый человек должен иметь возможность доступа к информационным и коммуникационным сетям. Мы подтверждаем нашу приверженность предпринимаемым в настоящее время усилиям по разработке и осуществлению последовательной стратегии, направленной решение данного вопроса. Мы также приветствуем то, что и промышленность, и гражданское общество все более склоняются к признанию необходимости преодоления этого разрыва. Мобилизация наших знаний и ресурсов в этой области является необходимым условием для урегулирования данной проблемы. Мы будем и далее стремиться к эффективному сотрудничеству между правительствами и гражданским обществом, чутко реагирующим на высокие темпы развития технологий и рынка.

10. Ключевой составляющей нашей, стратегии должно стать непрерывное движение в направлении всеобщего доступа для всех. Мы будем и далее:

содействовать установлению благоприятных рыночных условий необходимых для предоставления населению услуг в области коммуникаций:

изыскивать дополнительные возможности, включая доступ через учреждения, открытые для широкой публики:

уделять приоритетное внимание совершенствованию сетевого доступа, в особенности в отсталых городских, сельских и отдаленных районах;

уделять особое внимание нуждам и возможностям людей, пользующимся меньшей социальной защищенностью, людей с ограниченной трудоспособностью, а также пожилых граждан, и активно осуществлять меры, направленные на предоставление им более легкого доступа;

содействовать дальнейшему развитию "удобных для пользования", "беспрепятственных" технологий, включая мобильный доступ к сети Интернет, а также более широкое использование бесплатного, общедоступного информационного наполнения и открытых для всех пользователей программных средств, соблюдая при этом права на интеллектуальную собственность.

11. Стратегия развития информационного общества должна сопровождаться развитием людских ресурсов, возможности которых соответствовали бы требованиям информационного века. Мы обязуемся предоставить всем гражданам возможность освоить и получить навыки работы с ИТ посредством образования, пожизненного обучения и подготовки. Мы будем и далее стремиться к осуществлению этой масштабной цели, предоставляя школам, классам и библиотекам компьютерное оборудование, способное работать в режиме реального времени, а также направлять туда преподавателей, имеющих навыки работы с ИТ и мультимедийными средствами. Кроме того, мы будем осуществлять меры по поддержке и стимулированию малых и средних предприятий, а также людей, работающих не по найму, предоставляя им возможность подключаться к сети Интернет и эффективно ею пользоваться. Мы также будем поощрять использование ИТ в целях предоставления гражданам возможности пожизненного обучения с применением передовых

методик, в особенности тем категориям граждан, которые в противном случае не имели бы доступа к образованию и профессиональной подготовке.

**Содействие всеобщему участию**

12. ИТ открывает перед развивающимися странами великолепные возможности. Страны, которым удалось направить свой потенциал в нужное русло, могут надеяться на преодоление препятствий, традиционно возникающих в процессе развития инфраструктуры, более эффективное решение своих насущных задач в области развития, таких как сокращение бедности, здравоохранение, улучшение санитарных условий и образование, а также использование преимуществ быстрого роста глобальной электронной торговли. Некоторые развивающиеся страны уже достигли значительных успехов в этих областях.

13. Тем не менее не стоит недооценивать проблему мирового масштаба, связанную с преодолением существующих различий в области информации и знаний. Мы отдаем должное тому вниманию, которое уделяют этой проблеме многие развивающиеся страны. В действительности, все те развивающиеся страны, которые не успевают за все более высокими темпами развития ИТ, оказываются лишенными возможности в полной мере участвовать в жизни информационного общества и экономике. Этот вопрос особенно остро стоит в тех странах, где распространению ИТ препятствует отставание в развитии основных экономических и социальных инфраструктур, в частности энергетического сектора; телекоммуникаций и образования.

14. Мы признаем, что при решении этой проблемы следует учитывать разнообразие условий и потребностей, которое сложилось в развивающихся странах. Здесь не может быть "уравнительного" решения. И это в свою очередь говорит о той важной роли, которую должны сыграть развивающиеся страны, выдвигая собственные инициативы о принятии последовательных национальных программ с целью осуществления политических мер, направленных на поддержку развития ИТ и конкуренции в этой сфере, а также создания нормативной базы, использование ИТ в интересах решения задач в области развития и в социальной сфере, развитие людских ресурсов, имеющих навыки работы с ИТ, а также с целью поощрения выдвигаемых на локальном уровне инициатив и местного предпринимательства.

**Дальнейшее развитие**

15. Усилия по преодолению международной разобщенности в решающей степени зависят от эффективного сотрудничества между всеми участниками. Для создания рамочных условий для развития ИТ важную роль и в дальнейшем будут играть двустороннее и многостороннее сотрудничество. Международные финансовые институты, включая многосторонние банки развития (МДБ), особенно Всемирный банк, весьма пригодны для этой цели и могут разрабатывать и осуществлять программы, которые будут способствовать росту и борьбе с бедностью, а также расширять связи, доступ и обучение. Международная сеть телекоммуникаций, ЮНКТАД и ЮНДП и другие соответствующие международные фонды также могут сыграть важную роль. Центральной остается роль частного сектора в продвижении ИТ в развивающихся странах. Он может также существенно способствовать международным усилиям по преодолению цифрового разрыва. НПО, обладающие уникальными возможностями донести идеи до общественности, также могут способствовать

развитию человеческих и общественных ресурсов. ИТ глобальна по своей сути и требует глобального подхода.

16. Мы приветствуем уже предпринимаемые усилия по преодолению международного электронно-цифрового разрыва посредством двусторонней помощи в области развития и по линии международных организаций и частных групп. Мы также приветствуем вклад частного сектора в лице таких организаций, как Глобальная инициатива по ликвидации электронно-цифрового разрыва Всемирного экономического форума (ВЭФ) и Глобальный диалог бизнеса по вопросам электронной торговли (ГДБ), а также Глобальный форум.

17. Как отмечается в декларации о роли информационных технологий в контексте основанной на знаниях глобальной экономики, которая была принята Экономическим и Социальным Советом ООН (ЭКОСОС) на уровне министров, существует необходимость расширения международного диалога и сотрудничества в целях повышения эффективности программ и проектов в области информационных технологий совместно с развивающимися странами и сведения воедино "наилучшего опыта", а также мобилизации ресурсов всех участников для того, чтобы способствовать ликвидации электронно-цифрового разрыва. "Восьмерка" будет и далее содействовать укреплению партнерства между развитыми и развивающимися странами, гражданским обществом, включая частные фирмы и НПО, фонды и учебные заведения, а также международные организации. Мы будем также работать над тем, чтобы развивающиеся страны в партнерстве с другими участниками могли получать финансовое, техническое и политическое обеспечение в целях создания благоприятного климата для использования информационных технологий.

18. Мы договорились об учреждении Группы по возможностям информационной технологии (Группа ДОТ), чтобы объединить наши усилия в целях формирования широкого международного подхода. Группа ДОТ будет созвана в кратчайшие сроки для изучения наилучших возможностей подключения к работе всех участников. Эта группа высокого уровня в режиме тесных консультаций с другими партнерами и воспринимая потребности развивающихся стран будет:

активно содействовать диалогу с развивающимися 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, а также поощрения участия в глобальных сетях электронной торговли;

поощрять собственные усилия "восьмерки" в целях сотрудничества в осуществлении экспериментальных программ и проектов в области информационных технологий;

содействовать более тесному политическому диалогу между партнерами и работать над тем, чтобы мировая общественность больше знала о стоящих перед ней вызовах и имеющихся возможностях;

изучит вопрос о том, какой вклад вносит частный сектор и другие заинтересованные группы, например, Глобальная инициатива по ликвидации электронно-цифрового разрыва;

представит доклад по итогам работы нашим личным представителям до следующей встречи в Генуе.

19. Для выполнения этих задач группа будет изыскивать пути к принятию конкретных мер в указанных ниже 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 и другими партнерами;

- содействие более эффективному и широкому использованию информационных технологий в области развития, включая такие широкие направления, как сокращение бедности, образование, здравоохранение и культура;

- совершенствование системы управления, включая изучение новых методов комплексной разработки политики;

- поддержка усилий МБР и других международных организаций в целях объединения интеллектуальных и финансовых ресурсов в контексте программ сотрудничества, таких, как программа "InfoDev";

Улучшение технической совместимости, расширение доступа и снижение затрат:

- мобилизация ресурсов в целях улучшения информационной и коммуникационной инфраструктуры, уделение особого внимания "партнерскому" подходу со стороны правительств, международных организаций, частного сектора и НПО;

- 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;

- улучшение взаимодействия между сетями, службами и прикладными системами;

- поощрение производства современной информационно содержательной продукции, включая расширение объема информации на родных языках.

**Укрепление человеческого потенциала:**

- уделение повышенного внимания базовом образованию, а также расширению возможностей пожизненного обучения с упором на развитие навыков использования информационных технологий;

- содействие подготовке специалистов в сфере информационных технологий 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;

- создание сети государственных учреждений и институтов, включая школы, научно-исследовательские центры и университеты.

**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 информационных технологий для повышения эффективности их деятельности и расширения доступа к новым рынкам;

- обеспечение соответствия возникающих "правил игры" усилиям в сфере развития и укрепление способности развивающихся стран играть конструктивную роль в определении этих правил.

**Источник:** http://www.russianlaw.net/law/general/z8/?print=news_view.tpl (14.10.20011)

*АНДРЕЙ КРУТСКИХ*

# К ПОЛИТИКО-ПРАВОВЫМ ОСНОВАНИЯМ ГЛОБАЛЬНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основная озабоченность в сфере обеспечения международной информационной безопасности связана с возможностью применения информационно-коммуникационных технологий (ИКТ) в целях, несовместимых с задачами обеспечения международной стабильности и безопасности. Важнейшими угрозами здесь видятся враждебное использование ИКТ на уровне государств против информационных инфраструктур в политических, в том числе военных целях, преступная и террористическая деятельность в киберпространстве.

В современном мире происходит постепенная «информатизация» вооруженных сил и «интеллектуализация» традиционных вооружений. Информационное оружие становится важным элементом военного потенциала государств. Оно эффективно дополняет традиционные военные средства и в ряде случаев способно заменить их. В таких условиях Россия стала первым государством, которое на международном уровне подняло вопрос о появлении принципиально новых (информационных) угроз национальной и международной безопасности в XXI веке.

1

Рубеж XX – XXI веков стал периодом смены формы межгосударственных конфликтов: при помощи ИКТ нападения и агрессии могут осуществляться трансгранично, без привлечения армейских подразделений и использования традиционных вооружений и военной техники, с помощью негосударственных субъектов. Дестабилизация экономики, подрыв суверенитета и основ государственного устройства, нарушение нормального функционирования инфраструктур могут быть достигнуты за счет применения информационных средств. Вот почему эффективное обеспечение национальной и международной безопасности невозможно без укрепления международной информационной безопасности (МИБ), и прежде всего – за счет снижения угроз враждебного использования ИКТ.

С 1998 г. Россия продвигает идею налаживания международного сотрудничества по укреплению МИБ. Эта работа ведется параллельно по нескольким направлениям.

На двустороннем уровне в 1998–2006 годах были проведены *межведомственные экспертные консультации* с США, Китаем, Бразилией, ЮАР, Индией и другими странами. Эти встречи выявили близость позиций сторон по основным вопросам информационной безопасности. Договоренности о межгосударственном сотрудничестве в целях ее укрепления были впоследствии закреплены в совместных российско-американском, российско-китайском и российско-бразильском заявлениях.

Вопросам МИБ были посвящены *аналитические семинары*, проведенные, в частности, под эгидой Института ООН по проблемам разоружения и Международного комитета Красного Креста. По инициативе России проблематика МИБ рассматривалась *на высоком политическом уровне и многосторонней основе* – в «группе восьми», Шанхайской организации сотрудничества (ШОС), на Полномочной конференции Международного союза электросвязи (МСЭ), Всемирной встрече на высшем уровне по вопросам информационного общества, в рамках СНГ и Регионального содружества в области связи (РСС)[1]. В соответствующих итоговых документах были закреплены положения о наличии угроз для МИБ и о необходимости сотрудничества в интересах снижения их уровня.

Первым шагом в направлении организации эффективного международного взаимодействия в сфере МИБ стало предложение России, сделанное Вашингтону еще в 1998 году, подписать на уровне глав государств совместное заявление по проблематике международной информационной безопасности. В проекте документа отмечалось, что в современной ситуации в информационной сфере, с одной стороны, имеется потенциал

развития человечества через глобальную информационно-технологическую революцию, а с другой – присутствуют угрозы использования новых технологий в целях подрыва международной стабильности.

Подчеркивалось, что наличие новых угроз требует принятия превентивных мер, среди которых могут быть:

– согласование взглядов мирового сообщества на проблемы возможного использования информационных технологий в военных целях;

– определение основных понятий («информационное оружие», «информационная война»);

– выявление возможностей использовать информационные технологии для совершенствования существующих и создания новых систем оружия;

– рассмотрение вопроса о том, насколько целесообразно создать международную систему мониторинга угроз информационной безопасности;

– внесение вопроса о глобальной информационной безопасности на рассмотрение ООН и других ведущих международных форумов;

– создание международно-правового режима запрещения разработки, производства и применения особо опасных видов информационного оружия;

– выработка многостороннего договора о борьбе с информационным терроризмом и преступностью.

По мнению российской стороны, такое совместное заявление могло бы способствовать началу конкретного, всестороннего и целенаправленного обсуждения возникающих проблем. В итоге обсуждения этого предложения идея заявления по МИБ реализована не была. Однако обеспокоенность возникающими угрозами в этой сфере нашла отражение в Совместном российско-американском заявлении об общих вызовах безопасности на рубеже XXI века, подписанного президентами России и США по итогам Московского саммита 2 сентября 1998 года.

В этом заявлении было отмечено, что стороны согласились активизировать совместные усилия по противодействию транснациональным угрозам экономике и безопасности, включая преступления с использованием компьютерной техники и других высоких технологий. Россия и США признали «важность содействия положительным сторонам и ослабление действия отрицательных сторон происходящей информационно-технологической революции, что является серьезной задачей в деле обеспечения стратегических интересов безопасности наших двух стран в будущем»[2]. В документе было также сказано о том, что с общими вызовами безопасности на рубеже XXI века можно справиться только посредством мобилизации усилий всего международного сообщества. В случае необходимости мировое сообщество должно своевременно принимать эффективные меры по противодействию таким угрозам. Две великие державы впервые признали наличие проблемы информационной безопасности как таковой, обозначили реальные угрозы в этой сфере и высказались за комплексное, многостороннее сотрудничество для противодействия общим вызовам безопасности.

Дальнейшая работа по согласованию конкретных мер в интересах упрочения МИБ проводилась главным образом через механизм Организации Объединенных Наций. 23 сентября 1998 г. Генеральному секретарю ООН Кофи Аннану было направлено по этому поводу специальное послание министра иностранных дел России И.С. Иванова[3]. Генеральная Ассамблея ООН на протяжении ряда лет рассматривала на сессиях вопрос о роли науки и техники в контексте международной безопасности, разоружения и других областей, связанных с этим процессом. По мнению России, эта роль возрастает на современном этапе научно-технической революции с ее беспрецедентным уровнем развития и внедрения принципиально новых информационных технологий и средств телекоммуникаций.

В послании И.С. Иванова также констатировалось, что информационная революция проникает во все сферы жизнедеятельности общества, открывает перспективы для ускоренного развития мировой цивилизации и способствует увеличению созидательного

потенциала человечества. Формируется глобальное информационное пространство, в котором информация приобретает свойства ценнейшего элемента как национального, так и общечеловеческого достояния, его стратегического ресурса.

При этом, однако, была подчеркнута потенциальная, но серьезная опасность использования достижений в информационной сфере в целях, не совместимых с задачами поддержания мировой стабильности. Речь шла о необходимости соблюдения принципов неприменения силы, невмешательства во внутренние дела, расширения спектра прав и свобод человека.

Особый акцент был сделан на необходимости предотвратить появление конфронтации в информационной области, способной спровоцировать новый виток гонки вооружений в мире. В этой связи отмечалось, что речь идет о создании информационного оружия (ИО) и опасности возникновения информационных войн (ИВ). Принимая во внимание высокий уровень информатизации общества и одновременно уязвимость информационных структур, нельзя, однако, исключить возможности появления ИО, которое по своим разрушительным свойствам может сравниться с оружием массового поражения.

К посланию был приложен проект резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[4]. Проект был развитием данной резолюции: в нем отмечалось, что научно-технические достижения могут иметь гражданское и военное применение, причем содействие следует оказывать развитию науки и техники именно в гражданских целях. В проекте, в частности, содержалось приглашение всем государствам-членам Организации Объединенных Наций информировать Генерального секретаря ООН о своей точке зрения по вопросам использования информационных технологий в военных целях, уточнения понятий, враждебного или несанкционированного воздействия на информационно-коммуникационные системы и информационные ресурсы. Особо указывалось на важность диалога о целесообразности разработки международно-правовых режимов запрещения разработки, производства и применения особо опасных видов информационного оружия, а также борьбы с информационным терроризмом и криминалом, включая создание международной системы мониторинга угроз для безопасности глобальных информационно-коммуникационных систем.

Инициативные предложения России стимулировали обсуждения в Первом комитете Генассамблеи ООН, занимающимся вопросами разоружения и международной безопасности. Результатом этих дискуссий стала модификация проекта резолюции – в основном в части рекомендаций относительно информирования Генерального секретаря о точках зрения и оценках государств-членов Организации Объединенных Наций. 2 ноября 1998 г. пересмотренный проект был одобрен комитетом, а 4 декабря 1998 г. – принят без голосования (консенсусом) Генеральной Ассамблеей ООН (A/RES/53/70)[5].

Положения российского проекта об ограничениях использования информационных технологий в военных целях, определении понятий «информационное оружие», «информационная война», разработка режима запрещения информоружия в резолюции отражения не получили. Но ее политическое значение определялось тем, что впервые проблематика МИБ вошла в повестку дня широких международных обсуждений. В рамках этого документа были названы угрозы, связанные с возможностью разрушительного использования ИКТ.

В заявлении делегации США по мотивам голосования в Первом комитете было подчеркнуто, что одобрение резолюции означало вступление международного сообщества в процесс решения задач, которые включают многие взаимосвязанные факторы, не относящиеся обычно к компетенции Первого комитета. Речь идет о технических аспектах экономического сотрудничества и торговли интеллектуальной собственностью, правоохранительной деятельности, борьбе с терроризмом; традиционно подобные проблемы рассматривались в комитетах по экономическим, финансовым и правовым вопросам. При этом в заявлении Соединенных Штатов указывалось на полезность обсуждения действий не

только правительств, но и корпораций, предприятий и личностей, действующих в частном секторе.

Вплоть до 2005 г. российские резолюции по МИБ консенсусно принимались Генассамблеей ООН. Усилиями российской стороны положения резолюции развивались и наполнялись конкретными положениями. В принятой в 1999 г. резолюции Генеральной Ассамблеи ООН № 54/49 впервые была сформулирована «триада угроз» в сфере МИБ: применение информационных технологий в военных, террористических и преступных целях. Этот документ сформулировал, таким образом, *саму проблему незаконного использования информационно-коммуникационных технологий.*

В августе 1999 г. МИД РФ по согласованию с заинтересованными российскими ведомствами направил в Секретариат ООН новый документ – «Принципы, касающиеся международной информационной безопасности». Речь шла о варианте кодекса поведения государств в информационном пространстве, который был призван создать морально-политическую базу для международных переговоров под эгидой ООН по данной проблематике. В этом документе были варианты определения международной информационной безопасности, угроз информационной сферы, информационного оружия, информационной войны, международного информационного терроризма и преступности. В нем также говорилось о пяти базовых принципах международной информационной безопасности, роли права, обязательствах и ответственности государств в информационном пространстве, а также возможной роли ООН в контексте общих усилий в этой области.

План обеспечения МИБ, предложенный Россией, включал в себя определение признаков и классификацию информационных войн, информационного оружия и относимых к нему средств воздействия. Проект предусматривал меры по ограничению оборота информационного оружия, запрещению разработки, распространения и применения особо опасных видов ИО, предотвращению угрозы информационных войн. В документе говорилось также о запрещении использования ИТ во враждебных целях и, в частности, против согласованных категорий объектов. 20 ноября 2000 г. участники 55-й сессии Генассамблеи ООН единогласно приняли резолюцию № 55/28, в которой удалось сформулировать положение о необходимости изучения различных «концепций укрепления безопасности глобальных информационных и телекоммуникационных систем». *Это был уже шаг от констатации проблемы к поиску путей ее согласованного решения.*

В докладе Генерального секретаря ООН (A/56/164/Add.l от 3 октября 2001 г.) были названы основные угрозы личности, обществу и государству в информационном пространстве. К таким угрозам были отнесены:

– разработка и использование средств несанкционированного вмешательства в информационную сферу другого государства;

– неправомерное использование чужих информационных ресурсов и нанесение им ущерба;

– целенаправленное информационное воздействие на население иностранного государства; – попытки доминирования в информационном пространстве;

– поощрение терроризма;

– ведение информационных войн.

Принципиально важным было решение 56-й сессии Генассамблеи ООН от 29 ноября 2001 года, нашедшее выражение в ее резолюции № 56/19. На этой основе в 2004 г. была создана специальная группа правительственных экспертов для изучения проблемы международной информационной безопасности. В мандат группы вошло рассмотрение угроз в сфере информационной безопасности, возможных совместных мер по их устранению, а также проведение исследования концепций укрепления безопасности глобальных информационных и телекоммуникационных систем. В 2002 г. Генеральная Ассамблея ООН приняла решение о финансировании исследований на соответствующие цели, что позволило активизировать эту деятельность. *Исследовательская работа ООН была впервые поставлена на относительно систематическую основу.*

2

Важно отметить, что порой довольно радикальные первоначальные позиции отдельных государств (от отказа признать существование проблемы МИБ до призывов к полному и немедленному запрещению информационного оружия) в течение 1999–2002 годов стали умереннее и прагматичнее. Это произошло благодаря многостороннему диалогу, разъяснению взаимных подходов, а также объективному развитию международной ситуации, в которой большинство стран мира стало осознавать свою уязвимость перед вредоносными информационными воздействиями. Отсюда – естественное стремление государств переориентироваться с обсуждения абстрактных опасностей на решение конкретных задач.

Всего за шесть лет обсуждения проблематики МИБ в ООН были представлены 33 доклада разных государств, в том числе 4 документа Российской Федерации. Помимо России соответствующие документы направили США, Великобритания, Австралия, Украина, Белоруссия, Грузия, Швеция (от имени государств – членов Европейского Союза), КНР, Куба, Иордания, Мексика, Аргентина. Все эти доклады в конце концов признали наличие новой глобальной проблемы и необходимость обеспечения международной информационной безопасности.

При этом выявились различия в расстановке акцентов (военно-политическая, правовая, гуманитарная и другие составляющие), а также в предлагаемых методиках и форматах рассмотрения и решения проблемы. Официальные оценки продемонстрировали, что вопрос обеспечения информационной безопасности актуален для широкого круга стран. Решение данной проблемы невозможно, если не дополнять усилия отдельных стран созданием механизмов многостороннего сотрудничества.

8 декабря 2003 г. Генассамблея ООН консенсусом приняла новую резолюцию по информационной безопасности (AVR.ES/58/32), согласно которой начал действовать механизм формирования рабочей группы правительственных экспертов (ГПЭ). В ее состав на основе принципа справедливого географического распределения вошли представители Российской Федерации, США, Великобритании, Франции, Китая, Германии, Белоруссии, Бразилии, Мексики, Иордании, ЮАР, Мали, Индии, Малайзии и Республики Корея. Председателем группы был избран российский эксперт, что свидетельствовало о признании инициативной роли Российской Федерации в обсуждении данной проблематики. Сессии ГПЭ в дальнейшем проходили в Нью-Йорке (2004), Женеве (2005) и снова в Нью-Йорке (2005).

С первого дня выявились расхождения в позициях стран. Главным оппонентом России оказалась делегация США. Для американской стороны ИКТ являются мощным средством наращивания военного потенциала. ИО активно применялось американцами в ходе всех вооруженных конфликтов последнего десятилетия. Соединенные Штаты заинтересованы в сохранении свободы рук для военно-политического применения ИКТ и желают оставаться, по сути дела, вне сферы регулирования международного права.

В ходе переговоров американцы делали акцент исключительно на технологических аспектах защиты информационных сетей, борьбы с терроризмом и криминалом. Они выступали за исключение из текста доклада Генерального секретаря ООН формулировок ограничительного характера и указаний на военно-политическую составляющую МИБ.

Страны ЕС при этом выказывали озабоченность, прежде всего, относительно защиты от информационных угроз для экономики. Для развивающихся стран приоритетными оказались вопросы собственного информационного развития и сокращения «цифрового разрыва».

Все члены ГПЭ за исключением США признали:

1) способность ИКТ быть эффективным средством оказания негативного воздействия на гражданские и военные сферы государства;

2) наличие мощного разрушительного потенциала информационных агрессий;

3) возможность осуществления враждебных действий в информационном пространстве со стороны и государств, и негосударственных субъектов (преступники, террористы);

4) существование у государств потенциалов для тайного использования

киберпреступников;

5) необходимость принятия совместных усилий по снижению угроз и укреплению доверия в информационной сфере.

Однако решений принять не удалось: несогласие США сорвало консенсусное одобрение группой подготовленного проекта доклада Генерального секретаря ООН. В результате был принят «процедурный доклад», в котором лишь констатировался факт имеющихся разногласий.

Тем не менее проблематика МИБ заняла видное место в ходе международных дискуссий. Удалось не только сохранить обсуждение этой темы в Первом комитете, но также убедить в преимуществах коллективных мер ряд стран, связанных с США союзническими обязательствами. Несмотря на давление американской делегации, на Генассамблее ООН в декабре 2005 г. российские предложения по вопросам МИБ поддержали Япония, Израиль, Южная Корея, Австралия и Канада.

ГПЭ является важным многосторонним механизмом рассмотрения темы МИБ. Генассамблея ООН приняла решение создать в 2009 г. под эгидой Организации Объединенных Наций новую группу правительственных экспертов для дальнейшего рассмотрения вопросов МИБ. Ряд стран, ранее не участвовавших в работе группы, пожелали к ней присоединиться.

В 2006 г. на 61-й сессии Генассамблеи российская делегация снова предложила свой вариант резолюции по МИБ, выдвинув его в качестве коллективной инициативы ряда стран Организации Договора о коллективной безопасности и Шанхайской организации сотрудничества. За российский проект высказались 176 государств, против голосовали только США.

Согласование позиций государств относительно объектов обеспечения международной информационной безопасности велось и по линии подготовки «Хартии глобального информационного общества» на встрече лидеров стран «группы восьми» в июле 2000 г. на Окинаве (Япония). Тогда удалось зафиксировать:

(1) признание ИКТ в качестве основного фактора, формирующего общество XXI века;

(2) готовность содействовать переходу к информационному обществу;

(3) необходимость решения проблем, связанных с обеспечением безопасности использования этих технологий.

Для защиты инфраструктур жизнеобеспечения и информационных инфраструктур было решено привлекать представителей промышленности и негосударственных организаций, поскольку одни только правительства не способны обеспечить безопасность киберпространства. Особо была отмечена важность усилий каждого пользователя киберпространства для содействия обеспечению безопасности того участка пространства, которым он владеет или пользуется. Имелись в виду не только промышленные предприятия, но и организации всех секторов экономики, университеты, местные органы власти, а также граждане – пользователи системы Интернет.

Страны «группы восьми» пошли на закрепление в итоговом документе лишь вопросов целостности информационных сетей и пресечения преступлений в компьютерной сфере, обойдя военно-политическую составляющую МИБ. Проблема военного применения ИКТ государствами не была отражена, хотя военный аспект использования информационных средств является первостепенным.

Проблематика МИБ обсуждалась на Всемирной встрече на высшем уровне по вопросам информационного общества (ВВУИО). Первый этап этой встречи проходил в декабре 2003 г. в Женеве, второй – в ноябре 2005 г. в Тунисе. Важную роль в ее популяризации сыграла прошедшая в Марракеше (Марокко, сентябрь-октябрь 2002 г.) 16-я Полномочная конференция Международного союза электросвязи.

В качестве одной из мер, возможных для изучения в ходе подготовки к ВВУИО, страны назвали рассмотрение существующих и потенциальных угроз для безопасности информационных и коммуникационных сетей.

Участники ВВУИО также согласились внести вклад в реализацию усилий ООН, направленных на оценку состояния информационной безопасности, а также в рассмотрение вопроса о разработке (в долгосрочной перспективе) международной конвенции по безопасности в среде информационных сетей и сетей связи.

Нашедшие отражение в документах МСЭ формулировки по МИБ в дальнейшем легли в основу положений итоговых документов региональных конференций ВВУИО: общеевропейской (Бухарест, 7–9 ноября 2002 г.) и азиатской (Токио, 13–15 января 2003 г.). Включение формулировок по МИБ в декларации этих подготовительных встреч заложило основу для закрепления этой проблематики в повестке дня саммита и в его итоговых документах. В частности, был зафиксирован принцип универсального и недискриминационного доступа к ИКТ для всех стран, которые поддерживают деятельность ООН, направленную на предотвращение использования ИКТ в целях, несовместимых с задачами международной стабильности и способных оказать отрицательное воздействие на безопасность государств. Было сказано о необходимости предотвратить попытки использовать информационные ресурсы и технологии в преступных и террористических целях.

В качестве мер укрепления доверия и безопасности при использовании ИКТ авторы «Плана действий» выделяли (1) содействие сотрудничеству в рамках ООН в целях анализа реальных и потенциальных угроз в области ИКТ, (2) решение вопросов безопасности сетей, (3) изучение проблем совершенствованная законодательства, (4) проведение эффективных расследований и пресечение случаев ненадлежащего использования ИКТ. Говорилось о взаимопомощи в сфере профилактики компьютерных инцидентов, поощрении участия в деятельности ООН по укреплению доверия при использовании ИКТ.

В ходе работы конференции МСЭ в ноябре 2006 г. в Турции было уделено много внимания вопросам борьбы против использования ИКТ в целях разрушения. Участники встречи договорились создать специальный механизм – рабочую группу совета МСЭ – для проведения регулярных исследований по соответствующей проблематике и определению терминов, относящихся к технической сфере деятельности МСЭ. Группе было поручено представить доклад совету МСЭ в 2009 году.

3

Состоявшийся в Тунисе в ноябре 2005 г. второй этап Всемирной встречи на высшем уровне по вопросам информационного общества одобрил два итоговых документа: политический («Тунисское обязательство») и юридический («Тунисская программа для информационного общества»). Первый подтвердил и конкретизировал положения одобренной женевским этапом ВВУИО декларации принципов «Построение информационного общества – глобальная задача в новом тысячелетии»[6]. Второй документ определил механизмы реализации решений саммита, финансовые аспекты и вопросы управления Интернетом.

Главным и наиболее острым в ходе обсуждения стал вопрос о регулировании использования Интернета. Основная проблема заключалась в нежелании США отказаться от контроля над этой информационной сетью в пользу международного сообщества. Между тем она превратилась в основной элемент инфраструктуры глобального информационного общества. Наиболее жестко на интернационализации управления Интернетом и его ресурсами настаивали развивающиеся страны, которые поддержал Евросоюз. Россия выступала за то, чтобы ни одно правительство не играло определяющей роли в этом вопросе, предлагая сделать управление сетью многосторонним, прозрачным и демократичным с привлечением межправительственных и международных организаций.

Саммит поддержал эти принципы. Он принял важнейшее решение о начале процесса интернационализации управления Интернетом при обеспечении стабильности, безопасности и непрерывности функционирования этой глобальной информационной системы. Процесс стартовал в Афинах, где в октябре-ноябре 2006 г. было проведено первое заседание Форума

по вопросам управления Интернет (ФУИ). Второе собрание должно состояться в 2007 г. в Бразилии.

В Тунисе серьезное внимание уделялось вопросам безопасности. В итоговые документы саммита был включен предложенный Россией пункт о том, что ИКТ являются эффективным инструментом содействия делу мира, безопасности и стабильности. В документах также говорилось о недопущении злоупотреблений информационными ресурсами и технологиями. Помимо этого в них подтверждалась необходимость общего понимания участниками целей построения глобального информационного общества.

В итоговых документах второго этапа ВВУИО были отражены (не в последнюю очередь благодаря усилиям России) положения, подтверждающие значимость международного права, национального законодательства и суверенитета. Кроме того, российской делегации удалось отстоять положение о признании ведущей роли правительств в процессе, инициированном ВВУИО.

Новым этапом в мобилизации союзников ради выработки правил обеспечения МИБ на международной арене и организации практического сотрудничества в этой области стало заседание совета ШОС 15 июня 2006 года. Главы государств этой организации приняли заявление по международной информационной безопасности. Руководители России, Китая, Казахстана, Киргизии, Таджикистана и Узбекистана признали реальную опасность использования ИКТ против интересов безопасности человека, общества и государства в нарушение принципов равноправия и взаимного уважения, невмешательства во внутренние дела государств, мирного урегулирования конфликтов и неприменения силы. В заявлении ШОС подчеркивалось, что угрозы использования ИКТ в преступных, террористических и военно-политических целях могут реализовываться в гражданской и в военной сферах, приводя к тяжелым политическим и социально-экономическим последствиям.

Негативные последствия деструктивного применения информационных технологий преступниками и террористами, а также отдельными государствами для решения военно-политических задач могут затрагивать интересы многих стран, приобретая глобальный масштаб. Подобное использование ИКТ может вызывать катастрофы, сопоставимые по разрушительным последствиям с результатом применения оружия массового поражения. В таком контексте главы государств ШОС договорились о возможности проведения совместных мер по устранению информационных угроз при соблюдении норм международного права.

В октябре 2006 г. состоялось учредительное заседание Группы экспертов государств-членов ШОС по МИБ. В заседании приняли участие представители Республики Казахстан, Китайской Народной Республики, Киргизской Республики, Российской Федерации, Республики Таджикистан и Республики Узбекистан. Группе экспертов было поручено выработать к саммиту ШОС 2007 г. план действий и определить возможные пути решения проблемы МИБ в рамках компетенции стран-членов организации. Председателем группы консенсусом был избран российский эксперт.

По сути дела *страны ШОС, реагируя на угрозу переговорного тупика в соответствующей сфере на уровне ООН, заложили основу регионального сотрудничества в вопросах обеспечения информационной безопасности.* Политико-дипломатические последствия этого шага могут быть самыми разнообразными.

* * *

Разработка политико-правовой базы сотрудничества в обеспечении международной информационной безопасности идет медленно и крайне сложно. Международное сообщество сталкивается со старой проблемой – несовпадением интересов стран в вопросах кодификации деятельности в информационной сфере, которая, как уже общепризнано, стала важнейшей сферой обеспечения национальной и международной безопасности и в этом смысле крайне чувствительной областью взаимоотношений между странами.

Работа над договоренностями, тем не менее, поэтапно продолжается. Каждый

последующий документ опирался на предыдущий, параллельно принимались общие принципы деятельности государств в соответствующих областях. В случаях, когда достичь согласия относительно обязательных норм оказывается сложно, находятся иные, менее обязывающие и поэтому более приемлемые формы регулирования:

– кодексы поведения (например, по предотвращению распространения баллистических ракет);

– руководящие принципы (например, правила, публикуемые Группой ядерных поставщиков);

– меморандумы о намерениях (как это происходит в сфере нераспространения ракетных технологий).

Эти компромиссы ориентированы в некоторых случаях на достижение юридически обязывающих договоренностей. Такие типы документов можно было бы использовать как основу для будущей многосторонней конвенции о создании универсального режима международной информационной безопасности. Основой такого режима могло бы стать всеобщее обязательство не прибегать к действиям в информационном пространстве. Речь, таким образом, идет об отказе от действий, целью которых служит нанесение ущерба информационным системам, процессам и ресурсам другого государства с целью подрыва политической, экономической и социальной систем через психологическую обработку населения.

**Примечания:**

[1]Региональное содружество в области связи (РСС) было создано 17 декабря 1991 г. по инициативе Администраций связи 11 государств с целью широкого сотрудничества и проведения согласованных действий этих государств в области электрической и почтовой связи. В соответствии с Соглашением о координации межгосударственных отношений в области почтовой и электрической связи, подписанным правительствами государств – участников СНГ (Бишкек, 9 декабря 1992 г.), РСС одобрено как межгосударственный координирующий орган. РСС официально признано наблюдателем в Международном союзе электросвязи и Всемирном почтовом союзе – специализированных учреждениях ООН по связи. Высшим органом РСС является Совет глав Администраций связи. Постоянно действующим исполнительным органом РСС является Исполнительный комитет, который находится в Москве. Официальный сайт организации: http://www.rcc.org.ru (Прим. ред.).

[2]Дипломатический вестник МИД России. 1999. № 10. С. 13–14.

[3]UN Doc. A/C/1/53/3. 30 сентября 1998. С. 2–3.

[4]Ibid. С. 4–5.

[5]UN Doc. A/Res./53/70. 4 января 1999. С. 1–2.

[6]В документе подчеркивалась значимость ИКТ для преодоления «цифрового разрыва» в мире и необходимость сотрудничества на международном, региональном и национальном уровнях в целях построения глобального информационного общества.

**Источник:** http://www.intertrends.ru/thirteen/003.htm (01.10.2011)

*ДМИТРИЙ БАЛУЕВ*

# ПОЛИТИКА В ВОЙНЕ ПОСТИНДУСТРИАЛЬНОЙ ЭПОХИ

Об изменениях в природе военного конфликта «мировое сообщество» специалистов в области безопасности заговорило еще в годы «первой иракской войны» 1991 года. Однако в *политологическом смысле* говорить о реальности самих изменений до конца 1990-х годов было преждевременно. В самом деле, темпы внедрения собственно военных и военно-технических новаций ведения боевых действий существенно опережали динамику политических перемен в природе войны. В сущности, появление новых военных методов не сопровождалось соответствующими по значимости политическими последствиями. Американские исследователи признавали: «В 1991 г. США достаточно легко разгромили [иракскую] республиканскую гвардию и уничтожили всего за 100 часов четыре тысячи иракских танков, потеряв при этом лишь десять своих. Но преобразовать военную победу в политические изменения не удалось. Вот почему в последующие десять лет Соединенным Штатам пришлось проводить стратегию сдерживания Ирака»[1].

1

Явные сдвиги в понимании необычной природы новых войн стали происходить только после террористических актов 11 сентября 2001 года. Именно тогда начали трансформироваться американское внешнеполитическое мышление и взгляды американцев на войну. Осмысливая американский опыт, внимание политическим аспектам войн нового поколения стали уделять ученые и политики других стран. Но, естественно, в Соединенных Штатах перемены в политическом сознании были самыми заметными.

Наиболее характеры они были для самого президента Джорджа Буша и его ближайших советников[2]. В этом смысле наиболее броским (хотя не самым значимым) сдвигом был почти демонстративный разрыв республиканцев с превозносимым ими в 1990-х годах *изоляционизмом*. Именно он был основой их внешнеполитической доктрины на выборах 2000 года. Однако в 2001 г. администрация Буша без колебаний сделала выбор в пользу *интервенционизма, который предполагает* резкое повышение уровня глобальной военной активности. После событий сентября 2001 г. республиканцы, годами порицавшие администрацию У. Клинтона за ее политику «расширения демократии» и «вовлечения», приняли на себя такие военные обязательства, которые были немыслимы в правление демократов[3].

Поворотными пунктами в политическом использовании войн стали вторая афганская (2001-2002) и вторая иракская (2003-2005) кампании. С одной стороны, они продемонстрировали новые технологические возможности вооруженных сил США, позволяющие одерживать военную победу на поле боя сравнительно быстро и с минимумом потерь. С другой – обе кампании дали примеры того, как США борются с *типологически новыми* угрозами при помощи *старых* методов. Ведь провозглашенная Вашингтоном «глобальная война с международным терроризмом» не является войной в традиционном (для военной теории и военного искусства) смысле.

Обозреватели не раз писали, что обе кампании были средством отвлечь внимание американцев от внутриполитических и экономических проблем. Гораздо меньше специалисты развивали тему объективных трудностей на пути к адекватному осмыслению изменений в характере угроз и природы войны. Между тем, изменения реальности опережает обновление наших представлений о ней. Процесс осмысления перемен сложен и часто оказывается болезненным.

Хотя теоретическое осмысление новых тенденций отставало, в начале XXI века все же очевидна необходимость поставить проблему: как изменяется природа войны, если рассматривать последнюю в качестве варианта политического действия. «Война снова вернулась в политический арсенал». Точнее, она снова стала занимать в нем гораздо большее место, чем то, что было характерно для десятилетий «конфронтационной стабильности» в

биполярную эпоху. Реанимировался взгляд на войну как – прежде всего – на политический акт, а не простое столкновение вооруженных сил противников.

Для уяснения изменений природы войны и ее места в текущей мировой политике важно рассмотреть как минимум три группы факторов: технологические, информационно-психологические и собственно политические аспекты войны. Последнее подразумевает выявление места войн в современных международно-политических процессах. Уместно отметить, что большинство теоретических работ и документов внешнеполитического и военного планирования за рубежом и в России пока еще строятся на анализе – в основном – только первой группы факторов[4]. Информационно-психологические аспекты войны лишь в последнее время становятся предметом исследований, а ее политические аспекты вообще остаются за пределами внимания аналитиков.

Современные западные авторы чаще всего пишут об изменении роли силы в обеспечении безопасности, новых моделях применения военной силы в мировой политике и отличиях вооруженного конфликта в будущем от того, который был известен раньше[5]. Тезис об изменении природы конфликта, как правило, обосновывают ссылкой на так называемую *революцию в военном деле (РВД, revolution in military affairs)*.

Хотя об этой революции написано много[6], по-прежнему нет единого определения этого феномена. Исследователи по-разному видят его природу, направление развития и возможные последствия. Общим является лишь акцент на ее сугубо «технологичном» происхождении. Исходно в литературе фигурировал вообще весьма узкий по смыслу специальный термин «военно-техническая революция», который затем быстро трансформировался в более широкое понятие.

В зарубежной литературе существует рабочее определение этого понятия. Оно интерпретируется как *«военная и техническая революция, позволяющая применять технические нововведения в системе организации разведки, управления, контроля и связи». Такая революция связывается с появлением высокоточного оружия и, как следствие, новых операционных концепций, включая доктрины информационных войн и проведения совместных операций*[7].

Другая дефиниция предложена Управлением оценок Министерства обороны США. В этом случае РВД понимается как *значительное изменение в природе боевых действий, вызванное применением новых технологий, которое в свою очередь привело к пересмотру военной доктрины и операционных концепций и тем самым фундаментально изменило характер военных операций.* Как видно, второе определение игнорирует вопрос о сущности войны, которая представляет собой не только военные операции, а является комплексом взаимодействий политических целей, людских эмоций, культурных и этнических факторов и военного искусства. Авторы пентагоновской интерпретации не признают то обстоятельство, что технологии и технологические инновации при всей их важности остаются лишь инструментами достижения политических целей[8].

Впрочем оба определения РВД подразумевают изменения парадигмы, природы и способа проведения военных операций. Эти глубокие изменения существенно трансформируют ключевой параметр потенциала возможностей (core competency) доминирующего субъекта для использования силы или угрозы ее применения. Одновременно РВД может создавать новые ключевые параметры возможностей других субъектов.

Под *парадигмой* в данном контексте понимается модель, преобладающая при ведении определенного типа боевых операций. Так, во время наполеоновских войн парадигмой ведения боевых действий было использование пехоты, при поддержке и под прикрытием артиллерии, маневрирующей с целью войти в контакт с противником.

В предлагаемом анализе *ключевой параметр* означает главную, определяющую характеристику способности данной стороны реализовать свои задачи в конфликте. Например, возможность обнаружения наземных целей с воздуха и нанесения по ним ударов с использованием высокоточного оружия является ключевым параметром силовых

возможностей военно-воздушных сил (ВВС) США. А между мировыми войнами ключевым параметром военно-морских сил (ВМС) Соединенных Штатов была способность вести точный артиллерийский огонь на дистанции до 30 километров.

Под *доминирующим субъектом (dominant player)* мы понимаем вид вооруженных сил какой-либо страны, обладающий подавляющим превосходством в зоне военной операции, театра или кампании в целом. В кампаниях 2001-2004 годов доминирующим субъектом были ВВС США, поскольку они обладали безоговорочным преимуществом в воздушных боях и атаках с воздуха, которые были для соответствующих конфликтов ключевыми. В конце Второй мировой войны авианосные подразделения были доминирующим субъектом кампании на Тихоокеанском театре.

*Пространство боевых действий (dimension of warfare)* рассматривается как природно-географическая, антропогенная или иная среда, в которой ведутся боевые действия (земля, воздух, море, космос, киберпространство).

Наконец, *изменение парадигмы (paradigm shift)* означает смену базовой модели ведения боевых операций. Например, разрабатывая парадигму нанесения ударов силами *авианосных* соединений военно-морского флота (ВМФ), стратеги частично отказались от концепции использования «чисто» военно-морских сил – военных флотов, не имеющих в своем составе авианосцев[9].

РВД редко начинается доминирующими субъектами. Она часто заявляет о себе в конкретных ситуациях, давая преимущества той стороне, которая первой применила революционное нововведение. Нередко подобные перевороты случаются не там, где были сделаны новые технологические открытия, а там, где догадались, каким образом эти открытия можно эффективно применить.

Более того, РВД не всегда непосредственно связана с разработкой новых технологий. Например, использование североамериканскими колониями иррегулярных частей и ополченцев во время их войны за независимость от Великобритании (1775-1783) знаменовало собой революционное изменение в стратегии и тактике ведения боевых действий, хотя применением новой технологии или новых вооружений эти перемены не сопровождались.

В случае, когда «революция в военном деле» основана на технологических новшествах, она обычно является результатом внедрения одновременно нескольких технологий, а не применения какой-то одной. Не все РВД связаны с новым оружием. Например, распространение железных дорог в Европе и Америке в 1830-1850-х годах привело к резкому повышению стратегической мобильности[10], что сопровождалось сдвигами в стратегическом мышлении. Но собственно военно-технологических прорывов в этот период зафиксировано не было.

Американские эксперты полагают, что РВД последних пятнадцати лет характеризуется (1) бумом технологического развития, типичным для перехода от промышленной эпохи к информационной, (2) окончанием биполярной конфронтации и (3) сокращением военных бюджетов наиболее мощных держав прошлого века[11]. По мнению С. Метца, директора Института стратегических исследований при Колледже Вооруженных сил США, технологическо-организационный аспект современной РВД определяется четырьмя новациями[12]:

– приобретением ВС США способности к нанесению высокоточных ударов;
– существенным улучшением организации управления, контроля и разведки;
– появлением потенциала для эффективного ведения информационных войн;
– принятием на вооружение различных видов «несмертельного» оружия[13].

В исследованиях по заказам министерств обороны различных стран в последние годы сформулировано не менее пяти различных концепций использования новых возможностей РВД.

Во-первых, это теория *«бесконтактных» ударов с безопасного расстояния*. Идея заключалась в том, чтобы в интересах сохранения своего личного состава и техники избегать

непосредственного контакта с противником, нанося ему с большой дистанции удары, координируемые и направляемые высокочувствительными сенсорами и системами управления и наведения.

Во-вторых, существует концепция *информационной войны (information warfare)*, которая также изначально была предложена Э. Маршаллом, но затем развита американским ученым Р. Моландером[14]. Суть этого построения – концентрация усилий на информационной составляющей военной кампании с целью разрушить информационные системы противника, сохранив при этом свои.

В-третьих, в середине 1990-х годов появилась концепция *системы систем (system of systems)*, которую разработал американский адмирал У. Оуэнс. Ее суть заключалась в том, что связывание в единую систему подсистем сбора и обработки развединформации, управления, связи и контроля, высокоточных вооружений в целом более результативно, чем возможности каждой из этих подсистем.

В-четвертых, другой американский адмирал А. Цебровски представил концепцию *сетевой войны (net war)*. Новизна этой идеи состояла в требовании проведения боевых операций на «трех опорах», то есть с учетом слаженного использования возможностей трех уровней ведения кампаний: информационного, сенсорно-управляющего и уровня непосредственных боевых действий.

Наконец, в-пятых, появилась идея *кооперационных (cooperative) боевых действий*. Ее эффективность была продемонстрирована ВМФ США во время первой иракской войны (1991). Смысл нововведения заключался в использовании на театре военных действий географически изолированных платформ вооружений (weapon carrier) – крылатых ракет различного базирования, самолетов и беспилотных летательных аппаратов.

Хотя в США *имеются новые технологии (а также системы и устройства, использующие эти технологии), о разработке новой военной доктрины и соответствующей ей новой структуры вооруженных сил Соединенных Штатов речь пока не идет*. Имеются только операционные концепции, но они все еще проходят стадию тестирования[15].

В связи с формулированием военных доктрин, ориентированных на использование РВД, западные аналитики уделяют большое внимание вопросу о применении военной силы[16]. Лейтмотив их работ – мысль о необходимости свести к минимуму человеческие жертвы среди военнослужащих и гражданского населения. Американское общество демонстрирует довольно высокую степень нетерпимости к военным потерям – прежде всего, разумеется, своим. Возможно поэтому ряд авторов с оптимизмом оценивает потенциальный эффект от применения в конфликтах «несмертельного оружия». Американский ученый Э. Люттвак, например, заметил по этому поводу: «Если удастся должным образом модифицировать военное планирование, чтобы полностью использовать имеющийся технический потенциал, то станет возможно вернуться к методам ведения войн XVIII века, позволявшим избегать больших жертв и таким образом проводить почти бескровные интервенции»[17]. «Несмертельное оружие» может также облегчить интервенции на ранних стадиях конфликта.

Важное последствие РВД состоит в том, что она увеличивает разрыв в военных возможностях разных стран[18]. Государства, которые сумеют воспользоваться возможностями этой «революции», оставят далеко позади себя страны, неспособные поспевать за ней в силу консервативности, недостатка средств или отсутствия политической воли к самореформированию.

РВД позволяет передовым странам участвовать в конфликтах, не связанных с защитой их собственных жизненно важных интересов. Хотя снижается вероятность полномасштабного военного столкновения между самыми мощными государствами, но повышается угроза периферийных конфликтов, в которые могут быть вовлечены негосударственные акторы. Следовательно, при военно-политическом анализе возрастает необходимость учета интересов и прогнозирования поведения последних.

РВД может существенно изменить характер ведения боевых действий в конфликтах – как полномасштабных, так и малой интенсивности. Но подобные изменения вряд ли

автоматически повлекут за собой перемены в природе войны. РВД воплощает технологические трансформации в способах проведения военных операций. Однако технология сама по себе не определяет то, каким образом и ради чего военная сила используется политиками. Учет технологического аспекта проблемы не достаточен для теоретического осмысления феномена современной войны.

2

В анализ следует ввести также информационно-психологические составляющие. Внешнеполитические цели могут быть обеспечены не только военной силой, но и, например, экономическими мерами. Однако есть и другие аналитические инструменты. Мир, вступив в XXI век, требует «хирургически точного применения менее осязаемого, но более мощного оружия – знаний»[19].

Доминирование в информационной сфере дает возможность успешно достигать внешне- и внутриполитические цели. Обретение информационного превосходства чаще рассматривается ведущими державами как эффективное и перспективное средство, позволяющее добиваться политических целей в ситуациях, когда применение силы невозможно либо нецелесообразно. При этом информационное противоборство постепенно перемещается из военно-технологической сферы в область формирования мировоззрения при помощи методик политического манипулирования.

В настоящее время в обязательном порядке проводится пропагандистская поддержка военных операций. Лидирующие позиции здесь занимают Соединенные Штаты, в которых существует самая широкая в мире программа подготовки соответствующих специалистов. Основным местом их подготовки является Центр им. Дж. Кеннеди при Школе специальных операций в Форт Брэгге (John F. Kennedy Special Warfare Center and School at Fort Bragg, North Carolina)[20].

Основными задачами при достижении информационного превосходства являются «обрушивание» на противника «целенаправленно препарированной» информации или просто дезинформации, а также ограничение его возможностей получать достоверные сведения о планах и намерениях США и их союзников. Важной частью информационной войны является создание в собственной стране благоприятного общественного мнения вокруг осуществляемой операции. Спектр используемых средств варьируется от традиционной пропаганды и агитации до применения новейших технических средств.

Комбинация технологических новаций с методами информационно-психологического воздействия позволила разработать концепцию «операций, ориентированных на результат» (effects based operations). Смысл подобных операций состоит в возможности отказаться от ориентации на физическое уничтожение противника. Вместо этого упор делается на изменение поведения противника до такой степени, что он сам начинает психологически настраиваться на возможные выигрыши от капитуляции и отказа от вооруженного сопротивления. При этом новые средства воздействия не исключают использование силы, но главное внимание все же уделяется применению несиловых инструментов – психологического давления. Наряду с ними предусматривается использование дипломатии[21], экономических и политических воздействий[22]. Подобный подход, в сущности, тоже рассчитан на применение силы, однако не только с целью уничтожения вооруженных сил и материальной инфраструктуры оппонента, но также для воздействия на его психологическое состояние и даже мышление.

В принципе идея подобных операций не нова. Оценкой поведенческих мотиваций противника интересовался еще в начале XIX века немецкий стратег Карл фон Клаузевиц, подчеркивавший важность психологических аспектов войны. Целью военных действий, утверждал он, может быть и психологическое устрашение противника, а не только его физическое уничтожение.

В литературе выделяют несколько преимуществ операций, ориентированных на результат (ООР). *Первое* – чисто методологическое. Заложенный в логику ООР подход

позволяет сделать планирование военных операций более многоплановым, гибким и потенциально ресурсосберегающим. Эта методология прекрасно обеспечивает интеграцию военных и невоенных аспектов планирования.

*Второе* достоинство ООР – возможность эффективно осуществить выборку целей и установить соотношения их приоритетности. Этот подход позволяет наилучшим образом выявить слабые места противника путем анализа его системных возможностей. Он ориентирует на разрушение именно ключевых звеньев инфраструктуры противника и позволяет не уничтожать ее полностью. Считается, что таким образом легче проводить параллельные операции против избранных целей вместо того, чтобы поражать их одну за другой[23].

*Третья* сильная сторона ООР – способность оптимальным образом использовать все составляющие мощи своего государства: политические, экономические, военные и дипломатические. Это важно, поскольку полагаться на один единственный источник национальной мощи неразумно: ведь односторонность часто ведет к снижению эффективности кампании и облегчает адаптацию противника к нападению.

В литературе отмечается и *четвертое* достоинство подобных операций. Они стимулируют более тесное взаимодействие между теми, на кого возложено непосредственное командование боевыми операции и другими участниками обеспечения кампании. Таким образом, в условиях противостояния сложному противнику снижается вероятность ошибок и несогласованности.

Наконец, пятое преимущество состоит в том, что ООР лучше подходят к условиям ведения «сетевой войны»: теоретики подобных операций рассматривают противника как сложную и способную к адаптации систему.

Концепция ООР была довольно успешно обкатана во время информационных операций, сопровождавших вторую иракскую войну. Во время этой кампании психологическая война против Ирака велась с помощью 50 млн. листовок и сотен часов радио- и телетрансляций. Одновременно применялись стратегии подавления систем связи противника с целью подрыва эффективности работы иракской ПВО. В частности, ВС США заблокировали работу иракских средств связи на большинстве радиочастот, вынудив иракцев работать в предельно узком частотном диапазоне, который Соединенные Штаты могли полностью контролировать. Активно использовалась и дезинформация.

Правда, трудностей у американских военных в ходе иракской кампании 2003 года было достаточно. Это прежде всего относится к наземной части кампании.

С одной стороны, она выявила недооценку командованием коалиции роли природных условий и особенностей партизанской борьбы в условиях города. Американские и британские офицеры признавали, что пыльные бури и сопротивление иракцев в южных районах страны на неделю задержали наступление на Багдад. В особенности пострадали подразделения 101-й воздушно-десантной дивизии в районе Наджафа, которые вели боевые действия против Республиканской гвардии с помощью вертолетов «Апач».

А с другой стороны, нехватка пехотных формирований для оккупации и проведения зачисток городских районов вынудила американские войска обходить большие города. Фактически, союзники входили в них лишь для того, чтобы обеспечивать безопасность мостов и линий снабжения. Полный контроль над городами не был установлен и после того, как завершилась активная военная фаза кампании.

Кроме того, военные с большим трудом справлялись с непривычными для них боевыми задачами, поставленными в связи с политико-военными целями кампании. Основной задачей Вашингтона было добиться свержения режима Саддама Хусейна. Вот почему выбор целей в Ираке осуществлялся весьма специфическим образом.

Планируя воздушную составляющую кампании, американские военные стремились прежде всего уничтожить элитные иракские формирования и подразделения разведки. Авиаудары предполагалось наносить таким образом, чтобы максимально повысить вероятность уничтожения военных и политических руководителей Ирака, а также деятелей,

причисляемых к террористам и предположительно находящихся во время кампании на иракской территории. Такая приоритетность выбора целей противоречила декларировавшемуся ранее отказу Вашингтона от практики убийств зарубежных лидеров.

Правда, практика устранения отдельных вождей террористов складывалась еще при администрации У. Клинтона (1993-2000). В августе 1998 г. американские спецслужбы и военные попытались организовать с помощью ракет «Томагавк» покушение на Усаму бен Ладена. Однако оно оказалось неудачным. А после событий 11 сентября 2001 г. сенат и палата представителей Конгресса приняли совместную резолюцию, которая дала президенту США право «использовать необходимую силу» для ведения войны против терроризма. В результате правовое основание получили президентские директивы, разрешающие уничтожение предводителей террористов. Напомним, что именно на их основе в Йемене был уничтожен Абу-Синана Али аль-Харити, видный деятель «Аль-Каиды».

С тех пор поиск подобных «целей» непрерывно осуществлялся с помощью всех средств электронной разведки, а наведение на цель в режиме реального времени обеспечивалось силами специальной группы немедленного нацеливания (time-critical targeting cell), созданной в рамках отдела боевых операций Центра авиационных операций ВВС США. Опыт последних лет показал высокую эффективность такого поражения целей. Однако довольно быстро обозначились и проблемы. Зачастую политическая «санкция» на поражение той или иной цели запаздывала, и малая скорость принятия решений не соответствовала возросшим техническим возможностям разведывательных систем и средств управления огнем.

С военно-технологической точки зрения вторая иракская война проходила достаточно гладко. Реализованность ее политических целей – спорна. Краткосрочные военные цели кампании были достигнуты в соответствии с установками политического руководства США, в сжатые сроки и с минимальными потерями. Но на пути к долгосрочным политическим целям Вашингтон столкнулся с рядом трудностей. Даже военный потенциал Соединенных Штатов не обеспечил их осуществления – пока не удалось установить в Ираке тот режим, который казался оптимальным для американских интересов.

*Между тем вторая иракская война была фактически первой кампанией, полностью планировавшейся на базе концепции ООР. Но она показала, что технология сама по себе не гарантирует достижения искомых политических целей*. Возможно заново осознавая это, американские политологи стали чаще возвращаться к идеям Клаузевица. При этом, однако, они в большей степени опираются на их упрощенное толкование, которое было характерно для советского периода.

В свое время В.И. Ленин постарался «уравновесить» войну и политику, представить первую просто как одну из естественных форм второй. Не приемлющие коммунизм «ястребы» в нынешней республиканской администрации так же, как и он, полностью оправдывают войну, стараясь представить ее в глазах американского и мирового политического мнения как рядовое, обычное средство регулирования международных отношений. При этом сам К. фон Клаузевиц всегда рассматривал войну как крайнюю, предельную и в этом смысле исключительную фазу политической борьбы[24]. Парадоксально, но в американской администрации фактически преобладает ленинское толкование Клаузевица.

Однако войны в понимании самого немецкого стратега всегда велись для достижения политических целей, а не для военной победы самой по себе. При этом степень влияния политических соображений на военные операции менялась. Одной крайностью является ситуация, когда политические условия провоцировали начало боевых действий, затем приобретавших автономию и развивавшихся по логике, имеющей мало общего с первоначальными политическими целями. Другая крайность – случаи, когда политические соображения, влияя на боевые операции, мешали достижению военной победы. Но если полагаться на осмысление опыта иракской кампании, то можно заключить: простого *учета* политических целей военной кампании *не достаточно для достижения* полноценной

*политической победы*.

3

Уточнить представления об особенностях современной войны можно с помощью так называемого *фактора асимметрии*. Принятие концепции ООР американским военным планированием отражает некую важную тенденцию развития стратегической мысли США. Однако принципы этой концепции не могут быть в равной мере применимы ко всем, весьма разнообразным военным конфликтам. Соответственно сильно варьируются и методы обеспечения «выигрышного поведения». Их выбор во многом зависит от правильности нашего понимания военных угроз и угроз безопасности. В последнее десятилетие природа этих угроз меняется, в частности, оттого, что растет важность и многообразие так называемых асимметричных угроз.

Термин «асимметрия» привлекает все больше внимания. Однако используют его часто недостаточно точно. *Асимметрия означает отсутствие общей основы для сравнения*. В военно-политической сфере она проявляется в использовании асимметричных политических стратегий, ведении асимметричных боевых действий и появлении асимметричных угроз.

*Асимметричные политические стратегии* являются наиболее общим родовым понятием ситуаций, в которых «невоенные» методы используются для достижения военных целей, а информационно-психологические методики служат защите политических интересов. Пример такого рода – использование страхов гражданского населения (психологическое устрашение) для целей свержения правительства или компрометации международных союзов, в которых участвует государство.

*Асимметричные угрозы* нередко возникают, когда другая сторона ощущает опасность от превосходящего ее противника и не может ответить ему симметрично, то есть используя типологически те же силы и средства проецирования угрозы, которые использует тот. В самом общем виде *асимметричные боевые действия* построены на использовании «сравнительных преимуществ» одной стороны против «сравнительных уязвимостей» другой. Инструментами асимметричных (по отношению к операциям регулярных сил) боевых действий могут быть: (1) использование нерегулярными формированиями оружия массового поражения, баллистических или крылатых ракет, (2) применение информационных технологий или (3) перенесение боевых действий в нехарактерную для них среду (города, джунгли, высокогорье, пещеры).

В военной истории немало кампаний, выигранных вооруженными силами, которые имели схожие с противником (симметричные) возможности. Зато примеры асимметричных военных ответов сравнительно редки и, как правило, связаны с использованием (или планами использования) военно-технологических, операционных и тактических инноваций. Примером асимметричного военного ответа можно считать контрмеры СССР, предпринятые в ответ на американскую стратегическую оборонную инициативу в 1980-х годах, когда сравнительно дешевыми средствами подрывалась эффективность планируемой к развертыванию системы противоракетной обороны США.

Некоторые авторы считают примером асимметричных (по логике стратегического мышления) боевых действий ход германского наступления на Францию в 1940 году, проводившегося через незащищенную территорию Бельгии, а не посредством прорыва оборонительных укреплений на франко-германской государственной границе. Однако на самом деле ссылка на этот пример не убедительна. Германское наступление 1940 г. было все-таки в большей степени примером того, как отсутствие политической воли ведет к провалу кампании, чем случаем асимметричных боевых действий. Вермахт имел системы вооружений, однотипные с теми, что были на вооружение во Франции. На тактическом уровне между Францией и Германией существовали различия в степени подготовленности к эффективному использованию военного потенциала, а не асимметрия[25].

Примером явной операционной асимметрии (высокие технологии против обычных вооружений) можно считать американскую кампанию в Афганистане в 2001-2002 годах.

Американские вооруженные силы начали боевые действия с колоссальным технологическим превосходством (сенсоры, космические средства разведки и связи, высокоточное оружие и т.д.). Они имели возможность использовать сложнейшее электронное оборудование для координации действий собственных ВВС и сил специального назначения с наземными операциями Северного альянса, ставшего союзником Соединенных Штатов против талибов. Неоспоримое превосходство американских воздушных и наземных сил позволило и силам Северного альянса действовать практически без поражений. Ни талибы, ни «Аль-Каида» не могли противопоставить США и их союзникам ничего, сопоставимого с теми возможностями, которыми обладали американцы.

Рассмотрение асимметричных угроз правильно начинать с асимметрии интересов как наиболее важной их составляющей. Когда слабый противник имеет жизненный интерес, противоречащий нежизненно важному интересу более сильного государства, он получает достаточный стимул к тому, чтобы создать своему оппоненту асимметричную угрозу (что само по себе – асимметричная стратегия).

Подобные угрозы могут удержать более сильную державу от вмешательства в ситуацию, которая не угрожает ее жизненным интересам. Иногда асимметричная угроза способна ускорить вывод иностранных войск, просто сковать свободу действий более сильного государства или уменьшить его волю к вмешательству в чужие дела.

На рабочем уровне американские военные определяют асимметричные угрозы как попытку нейтрализовать или ограничить силовые преимущества США путем нанесения ударов по избранным уязвимым позициям Соединенных Штатов с помощью методов, не типичных для действий американских вооруженных сил.

Есть и более конкретное истолкование, которое подразумевает воздействие с использованием слабых тактических или операционных воздействий на уязвимые точки США. Цель таких акций – достижение непропорционально мощного эффекта, позволяющего подавить волю Соединенных Штатов или выполнить поставленные более слабой стороной задачи.

Асимметричные угрозы могут использоваться не обязательно слабыми странами. Аналитики Народно-освободительной армии КНР опубликовали серию исследований, в которых ведение асимметричных боевых действий рассматривается как один из ключевых средств достижения победы в будущих конфликтах (военных или иных) с Западом. В Китае разрабатываются технологии информационной войны, включая компьютерные вирусы, целью которых является ослабление информационной и управленческой инфраструктуры противника[26]. Важно то, что асимметричные стратегии могут быть нацелены на психологические манипуляции, посредством которых возможно компенсировать недостаток других ресурсов. Эффект от применения подобных методов может быть как тактическим, так и стратегическим.

В 1990-х годах западные эксперты по стратегии отчасти переключили внимание с *«войн по необходимости» (wars of necessity) на «войны по выбору» (wars of choice)*. Первые связаны с отражением угроз для выживания государства, вторые возникают при необходимости защиты не основных (второстепенных) интересов[27].

В современной ситуации «войны по выбору», как правило, ведутся под тем или иным предлогом в отношении слабых государств. Ядерные державы, да и западные страны в целом, фактически уже не находятся под угрозой «войн по необходимости», вызванных прямыми угрозами их существованию. Сознавая свою огражденность от жизненных угроз, они с большей или меньшей легкостью принимают решения о вступлении (если обстоятельства к тому вынуждают) в «войны по выбору», которые если и угрожают их интересам, то не жизненным[28], а основным или даже второстепенным. В этом смысле все «гуманитарные интервенции» – типичные «войны по выбору». Однако формально или неформально инициатором подобной войны может стать и более слабая сторона, имеющая неадекватное представление о соотношении своих сил с возможностями потенциальных противников.

Ведение «войн по выбору» отличается от ведения «войн по необходимости» тем, что в первом случае принять решение о начале войны труднее. Ведение боевых действий – дорогостоящее мероприятие, а его последствия не всегда предсказуемы. В принципе большинство государств до 1991 г. довольно явно тяготело к уклонению от прямых военных столкновений без крайней необходимости. Агрессия Ирака против Кувейта в этом смысле воспринималась как «чудовищная аномалия», а вовсе не норма. Но впоследствии модель международного поведения стала меняться. Чувствовавшие себя более сильными, члены НАТО стали прибегать к военной мощи чаще, смелей и откровенней, а все остальные страны мира, соответственно, стали относиться к ним подозрительней.

По-видимому, американские разработки проблематики «мягкой безопасности» (которые сегодня могут показаться в известном смысле новаторскими) в психологическом и политическом отношениях уходят корнями как раз к историческому опыту «зрелой биполярности» (1962 - 1991). Они отражают преломленное либералами-реалистами понимание опасности перерастания конфликтов из-за второстепенных интересов в полномасштабную катастрофу с участием ядерных держав[29].

Однако в последние пять лет военная сила вернула себе роль едва ли не ключевого инструмента межгосударственных отношений, в том числе отношений между государствами и негосударственными акторами (террористические сети). Правда, как отмечалось выше, традиционное использование военной силы против нетрадиционного противника не всегда может дать желаемый результат.

Асимметричные угрозы требуют совершенно новых стратегий противодействия им. На первое место выходит информационно-психологический аспект войн. Собственно военная победа становиться менее значимой, чем ее образ и «войны ради нее», который удается утвердить в СМИ и сознании общества. Чисто «технические» победы по-прежнему эффективны тактически, но они не гарантируют достижения стратегических, долгосрочных целей войны, которые по своей сути всегда являются политическими. *Военная победа США во второй иракской войне вполне очевидна. Но одновременно того же нельзя сказать не только о войне против терроризма, но даже о кампании за утверждение «иракской демократии»*. Реальная победа явно не соответствует победе ожидаемой.

В современных стратегических исследованиях требуется четче различать войны между государствами *(bellum)*, а также войны между государствами, с одной стороны, и субъектами, не имеющими легитимного государственного статуса *(guerra)* – с другой стороны[30]. Для конфликтов второго типа необходима особая стратегия[31].

Первой стадией выработки стратегии для конфликта типа *guerra* может быть уточнение его сути. Для этого стоит на время перестать думать о терроризме как о чем-то цельном и монолитном. Взамен надо сосредоточить внимание на изучении фактуры – исследовании конкретных актов террора, поведения и характеристик самих террористов, их целей, типа войны, которую они ведут. Только потом можно рассуждать о том, какого рода стратегия применения силы может быть против них эффективной.

Не ясно, в чем должны состоять особенности глобальной войны против терроризма, каковы оптимальные параметры ее ведения. Администрация США пока смогла лишь обозначить круг своих «врагов» в такой войне: государства-изгои, распространители ОМП, террористические организации (действующие в пределах отдельных стран, регионов или всего мира), отдельные террористы, наконец, «неудавшиеся государства», которые в силу слабости могут независимо от их воли использоваться «террористическими сетями».

К сожалению, такой перечень нивелирует различия между государствами-изгоями и террористическими организациями, хотя первые и вторые в корне различаются по характеру уязвимости перед лицом внешней военной мощи. Террористические организации – это конспиративные, негосударственные объединения, для которых лучшей защитой является отсутствие государственности. «Государства-изгои» как суверенные государства имеют территорию, население, инфраструктуру. Поэтому в отличие от террористических организаций они могут быть объектом традиционного сдерживания или военного нападения.

Рассмотрение их в одной классификационной категории ведет к путанице в прикладном анализе, что отчасти препятствует выработке эффективной антитеррористической политики.

Несмотря на неплохой тактический результат военного планирования во второй иракской войне и широкое использование в ней информационно-психологических воздействий, недооценка асимметричности угроз, с которыми столкнулись американские военные и гражданские оккупационные власти, привела к множественным неточностям в постановке задач этой войны в целом. Политические и военные цели кампании оказались во многом взаимоисключающими. К примерам подобной взаимоисключительности можно отнести цели уничтожения режима С. Хусейна и, например, обеспечения безопасности иракских нефтепромыслов. Обе были обозначены администрацией Буша как приоритетные[32]. При этом часть политических и военных целей была вообще недостижима. Ведь те и другие ставились не на базе достоверной разведывательной информации, а на основе конъюнктурных политико-идеологических установок правого крыла Республиканской партии и его представителей в «команде Буша»[33].

Заведомая недостижимость демонстративно заявленных политических целей Вашингтона обусловила стремление администрации задать иракской кампании жесткое информационно-пропагандистское сопровождение в СМИ. Инструментарий политико-психологического манипулирования при этом использовался в отношении как населения Ирака, так мирового общественного мнения. Фактически образ второй иракской войны оторвался от ее реального протекания, приобрел самостоятельное значение, начал «саморазвиваться» вне прямой связи с тем, что на самом деле происходило в Ираке и вокруг него. Возник феномен *«реальной виртуальности», под которой комментаторы стали понимать ситуацию, когда освещение и восприятие какого-то события оказалось политически и социально важнее, чем само это событие.*

Аналитики в связи с этим замечали, что стало реально возможным создание в СМИ образов несуществующих событий (в том числе *фиктивных военных конфликтов*), которые будут считаться реальными и порождать поэтому вполне реальные политические последствия.

* * *

Революция в военном деле в ее технологических проявлениях действительно меняет характер военных операций как в масштабных конфликтах, так и в войнах малой интенсивности. Но связанные с РВД изменения в системе боевых действий не влекут за собой автоматически изменений природы военного конфликта. Сама технология мало влияет на то, каким образом военная сила используется в политике. Рассмотрения только технологического фактора недостаточно для теоретического осмысления политических аспектов современной войны и тем более выработки практических рекомендаций для военного планирования.

Большинство важнейших систем вооружений США (да и других ведущих держав, включая Россию) создавалось во времена «холодной войны» и поэтому недостаточно приспособлено для борьбы с асимметричными угрозами, ведения боевых действий в городских условиях, когда противники и союзники находятся в тесном и нелинейном соприкосновении друг с другом. Подобные системы вооружений также плохо приспособлены к ведению боевых действий в условиях смешения гражданского населения с регулярными и нерегулярными вооруженными формированиями противника.

Ввиду роста числа военных конфликтов локального характера, важно принимать во внимание, что высокотехнологичные вооружения могут быть применены далеко не всегда. Целью в подобных конфликтах обычно бывает не разгром (уничтожение) противника или захват его территории, а изменение его политики. При этом военные операции, направленные на достижение политических целей, могут и должны сильно отличаться от операций, ориентированных лишь на военную победу. Это позволяет переосмыслить вопрос об оптимальной структуре вооруженных сил для «средних» региональных держав. Для

многих из них может быть достаточным ограничиться содержанием вооруженных сил, не предназначенных для уничтожения возможного противника, но способных вынуждать его при необходимости идти на определенные политические уступки без ведения полномасштабной войны на уничтожение. При наличии на рынке соответствующих технологий даже скромные военные бюджеты могут оказаться «достаточными» для поддержания обороноспособности, понимаемой подобным образом.

Переход к высоким («бескровным» для американских военнослужащих) технологиям ведения боевых действий сопровождался возникновением нехватки боеспособных пехотных частей для оккупации территории побежденного противника в условиях враждебности местного населения. Вот почему уместно ожидать попыток США использовать вооруженные силы и полицейские формирования союзных государств («миротворческих контингентов») или многонациональные силы под руководством американских командующих для выполнения политических задач после завершения боевых действий. Заметна и тенденция к «приватизации» военно-силовых полномочий государств[34]: стало распространяться (не афишируемое Вашингтоном) использование гражданских подрядчиков в целях обеспечения правопорядка в Ираке. Государство оказывается заинтересованным в снятии с себя части функций, связанных с использованием военной силы[35].

Возрастает интерес к использованию асимметричных способов ведения боевых действий, которые становятся новым путем достижения военно-политических целей. В данном случае асимметричные боевые действия – это использование одной из сторон неожиданной тактики, оружия с целью или нанести политическое поражение противнику, или уменьшить его превосходство вплоть до полной его нейтрализации. Призванные оказать воздействие на политические намерения противника, подобные действия могут компенсировать недостаток материальных, технологических и иных ресурсов.

Хорошо изученные стратегические концепции прежних эпох находят в современных условиях более ограниченное применение, чем прежде. Они не учитывают возникновение нового класса конфликтов – войн между государствами и транснациональными негосударственными субъектами (аморфными глобальными сетями, прямо не привязанными к системе межгосударственных отношений). Для конфликтов нового типа требуются типологически новые стратегии.

Растет значение фактора информационного превосходства как наиболее эффективного и перспективного средства достижения военно-политических целей. Роль этого инструмента может быть особенно значительна в ситуациях невозможности либо нецелесообразности использования традиционных вариантов военного вмешательства.

Становится технически возможным и экономически оправданным целенаправленное воздействие на процесс выработки потенциальным противником его ключевых военно-политических решений путем манипулирования информационными потоками, доступ к которым он стремится получить, или, наоборот, в которые он может быть искусственно погружен независимо от своей воли.

Происходит становление принципиально нового типа военных *«операций, ориентированных на результат»*, целью которых как раз и является давление на противника с целью побудить его изменить свою политику и поведение. Война перемещается (вернее – возвращается) из сферы собственно военного планирования в сферу политики. Заметен процесс (ре)интеграции военных инструментов во внешнеполитический арсенал ведущих государств и – что принципиально – негосударственных игроков международной политики.

Военные инструменты меняют свою природу в силу технологических новшеств и заимствования методов их применения из «невоенных» сфер деятельности. Применение военных средств все тесней увязывается с использованием невоенных, среди которых главным становится политическое манипулирование с учетом всей мощи современных информационных технологий. Наконец, растет количество закрытых разработок всевозможных вариантов асимметричного, оригинального, непредсказуемого применения самых разнообразных сочетаний военных и невоенных средств.

## Примечания:

[1]*B. Zellen.* Rethinking the Unthinkable: Nuclear Weapons and the War on Terror // Strategic Insights. 2004. Volume III. Issue 1.

[2]*T. Donnelly.* Underpinnings of the Bush Doctrine. National Security Outlooks / American Enterprise Institute for Public Policy Research, February 2003.

[3]*J.J. Wirtz, J.A. Russel.* US Policy on Preventive War and Preemption // Nonproliferation Review. Spring 2003. P. 113.

[4]Осмысление теоретических аспектов безопасности и войны в отечественной литературе последних пятнадцати лет тревожит и удручает. Публикации русских авторов в основном либо касаются исключительно конкретных вопросов (распространение ОМП и соответствующих технологий), либо представляют собой «сиюминутные» комментарии для газет или интернет-изданий по вопросам военной политики США и российско-американских диалогов в связи с военно-политической проблематикой. Нового поколения фундаментальных монографических работ, в которых бы в сколько-нибудь цельном виде анализировались сдвиги в представлениях о международной безопасности и роли войны в ее обеспечении, в России сегодня просто не существует. В университетах студентов учат по выходившим еще в советские годы обобщающим книгам А.Г. Арбатова, А.А. Кокошина и немногих других авторов и монографиям иностранных ученых, прежде всего – американских. Правда, нужно упомянуть новую монографию А.А. Кокошина «Стратегическое управление» (М.: РОССПЭН, 2003), однако ее содержание лишь отчасти затрагивает тему настоящей статьи. Этот же автор в 2004 г. опубликовал небольшую информативную работу «О политическом смысле победы в современной войне» (М.: УРСС, 2004). После длительного перерыва на русском языке вновь появились серьезные обобщающие статьи А.Г. Арбатова (Ядерное сдерживание и распространение: диалектика «оружия судного дня» // Мировая экономика и международные отношения. 2005. № 1). Склонность к теоретическим обобщениям на тему международной безопасности заметна в публикациях А.В. Фененко (Проблематика ядерной стабильности в современной зарубежной политологии // Международные процессы. 2004. № 3). Некоторые частные аспекты теории безопасности затрагиваются в новой совместной монографии Института проблем международной безопасности РАН и журнала «Международные процессы» (Мировая политика: теория, методология, прикладной анализ / Отв. ред. А.А. Кокошин, А.Д. Богатуров. М.: УРСС, 2005), а также в одной из наших работ (Балуев Д.Г. Личностная безопасность: международно-политическое измерение. Нижний Новгород: Изд-во ННГУ, 2004).

[5]*H. Sicherman.* Observations on the War // American Diplomacy. 2004. Vol. IX. No 1.

[6]См., например: *F. Kendall.* Exploiting the Military Technical Revolution. A Concept for Joint Warfare // Strategic Review. Spring 1992. P. 23-30; *M. Mazarr.* The Revolution in Military Affairs: A Framework for Defense Planning / Strategic Studies Institute, US Army War College, Carlisle Barracks, Pennsylvania. June 10, 1994; *A. Krepinevich.* Cavalry to Computer: The Pattern of Military Revolution // The National Interest. Fall 1994. P. 30-42; *M. Libick, J. Hazlett.* The Revolution in Military Affairs // Strategic Forum. No 11. Washington: Institute for National Strategic Studies, National Defense University, 1994; *M. Libicki.* Information and Nuclear RMAs Compared // Strategic Forum. No 82. Washington: Institute for National Strategic Studies, National Defense University. June 1996; *M. Libicki.* Illuminating Tomorrow's War // McNair Paper 60. Washington, 1994; *J. Barnett.* Future War: An Assessment of Aerospace Campaigns in 2010. Alabama: Air University Press, Maxwell AFB, 1996; *C. Gray.* The Changing Nature of Warfare // Naval College Review. 1995. Vol. XLIX. No. 2. P. 7-22.

[7]Past Revolutions Future Transformations: What Can the History of Revolutions in Military Affairs Tell Us About Transforming the U.S. Military? // MR-1029-DARPA, RAND, 1999. P. 8. Под «совместными операциями» в военных исследованиях, как правило, понимаются десантные, противодесантные, воздушные, противовоздушные, десантно-штурмовые операции и операции мобильных сил.

[8]*E. Tilford.* The Revolution in Military Affairs: Prospects and Cautions / Strategic Studies Institute, US Army War College. June 23, 1995. P. 1.

[9]Past Revolutions Future Transformations. P. 10.

[10]Подробнее об исторической перспективе революций в военном деле см.: *E. Sloan.* The Revolution in Military Affairs: Implications for Canada and NATO. McGill-Queen's University Press, 2002. P. 18-32.

[11]*E. Tilford.* Op. cit. P. 2.

[12]*S. Metz, J. Kievit.* Strategy and the Revolution in Military Affairs: From Theory to Policy / Strategic Studies Institute, US Army War College. June 23, 1995. P. V.

[13]Nonlethal Weapons and Capabilities. Report of an Independent Task Force Sponsored by the Council on Foreign Relations. New York: Council on Foreign Relations, 2004.

[14]*R. Molander, A. Riddile, P. Wilson.* Strategic Information Warfare / RAND, MR-661-OSD, 1996.

[15]Past Revolutions Future Transformations. P. 83.

[16]Наиболее показательным примером может служить: *Браун С.* Сила в инструментарии современной дипломатии // Международные процессы. 2004. № 2.

[17]*E. Sloan.* Op. cit. P. 19-20.

[18]*T.G. Mahnken, J.R. FitzSimonds.* Revolutionary Ambivalence: Understanding Officer Attitudes toward Transformation // International Security. 2003. Vol. 28. Issue 2.

[19]*R.L. Paarlberg.* Knowledge as Power: Science, Military Dominance, and U.S. Security // International Security. 2004. Vol. 29. Issue 1.

[20]Jane's Sentinel Security Assessment - North America / Jane's Information Group, 2004.
[21]*N. Kralev.* The Conduct of Diplomacy: Diplomacy Adapts to New Threats // American Diplomacy. 2004. Vol. IX. No 2.
[22]*J. Ho.* The Advent of a New Way of War: Theory and Practice of Effects Based Operations Singapore / Institute of Defense and Strategic Studies. Working Paper. December 2003. No 57. P. 2-3.
[23]Ibid. P. 6.
[24]Подробнее см. предисловие к: *Karl von Clausewitz.* War, Power and Politics / Translated and Edited with an Introduction by Edward Collins. Chicago: Henry Regnery Company, 1968. Автор благодарит А.Д. Богатурова за указание на эту публикацию.
[25]*M.C. Meigs.* Unorthodox Thoughts about Asymmetric Warfare. Parameters. Summer 2003. P. 6.
[26]*D. O'Brien and S. Nusbaum.* Intelligence Gathering on Asymmetric threats // Jane's Intelligence Review. October 2000. P. 52.
[27]*L. Freedman.* The Future of Military Strategy // Brassey's Defence Yearbook - 1996. Brassey's, 1996. P. 7.
[28]Под «жизненно важными интересами» мы понимаем совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.
[29]*J.S. Nye.* Soft Power: The Means to Success in World Politics. New York: Public Affairs, 2004.
[30]*S. Kalyanaraman.* Conceptualization of Guerrilla Warfare // Strategic Analysis: A Monthly Journal of the IDSA. April-June 2003. Vol. XXVII. No 2.
[31]*R.D. Worley.* Waging Ancient War: Limits on Preemptive Force / US Army War College, Strategic Studies Institute. February 2003. P. 1.
[32]*T. Donnelly.* The Meaning of Operation Iraqi Freedom. National Security Outlooks. American Enterprise / Institute for Public Policy Research, June 2003.
[33]Подробнее см.: *D. Byman.* Constructing a Democratic Iraq: Challenges and Opportunities // International Security. 2003. Vol. 28. Issue 1.
[34]Подробнее см.: *Балуев Д.Г.* Приватизация военно-силовых функций государства: каковы перспективы? // Мировая экономика и международные отношения. 2004. № 3. С. 64-70.
[35]*Косолапов Н.А.* Круговорот насилия в социальных структурах // Мировая экономика и международные отношения. 2004. № 3. С. 73.

**Источник:** http://www.intertrends.ru/nineth/002.htm (01.10.2011)

*СУДОРГИН О. А.*

# СОВРЕМЕННАЯ ИНФОРМАЦИОННАЯ ПОЛИТИКА ГОСУДАРСТВА: МИРОВОЙ ОПЫТ И РОССИЙСКАЯ ПРАКТИКА

**Автореферат (фрагмент)**

диссертации на соискание ученой степени доктора политических наук

Специальность 23.00.02 – политические институты, процессы и технологии

***Москва – 2011***

## I. Общая характеристика работы

Актуальность обращения к анализу информационно-политической проблематики вызвана рядом обстоятельств:

1. Во многих современных социумах произошли кардинальные изменения в области информационных технологий, совершился качественный скачок в производстве, хранении, накоплении, переработке и передаче информации. Но на практике это означает, что информационное пространство как объективно, так и субъективно используется для реализации общественных и политических целей, влияет на политику, ускоряя процесс принятия социально значимых решений и во многом трансформируя политический процесс. Фактически в современных информационных социумах постоянно ускоряются процессы принятия политических решений, повышается транспарентность функционирования власти, а граждане и их организации получают больше возможностей участвовать в управлении обществом. Граждане за счет создания социальных сетей всё активнее общаются друг с другом, минуя и государственное участие, и государственный контроль.

2. Информационная сфера все в большей степени становится системообразующим фактором жизни социума, а Интернет все активнее влияет на состояние политической, экономической, социальной и других сфер общественной жизни. При этом во всех ее сферах появляется и расширяется виртуальный сегмент, в который включаются все больше и больше людей, органов, организаций и институтов. Вместе с тем в различных государственных институтах и органах власти пока не сформировались корпоративные сети, подобные Интернету (хотя в бизнес-структурах такие сети созданы и успешно функционируют). Сетевой принцип управления пока не стал основой формирования и реализации государственной политики в современной Российской Федерации.

3. На рубеже веков и тысячелетий в современных государствах значительной степени изменилась структурная доминанта сферы и средств массовой информации. В конце 80-х – начале 90-х годов XX века мир масс-медиа представляла, прежде всего, печать – газеты и журналы. В настоящее же время наиболее содержательно и функционально разносторонним средством взаимодействия и распространения информации является Интернет и другие информационные технологии (мобильная связь). Но и эти информационные средства быстро устаревают. Прогнозируется, что развитие беспроводных сетей стандарта 802.11 и технологии VoiceOverIP в ближайшие 10-20 лет приведет к окончательной интеграции традиционных коммуникативных каналов и Интернета, создав глобальную информационную среду, удовлетворяющую критерию «любая информация в любом месте в любое время».

4. Отечественная политическая элита и руководство российского государства стремятся быть адекватными складывающимся реалиям информационного общества. В начале третьего тысячелетия в нашей стране была принята и реализовывалась федеральная целевая программа «Электронная Россия», многие государственные услуги переводятся в электронный вариант, была осуществлена компьютеризация и интернетизация средних и высших учебных заведений и т.д. На федеральном уровне в настоящее время создан президентский Совет при Президенте РФ по развитию информационного общества в Российской Федерации, подготовлен проект долгосрочной федеральной целевой программы «Информационное общество (2011-2018 годы)». В то же время многие политики, ученые и эксперты отмечают отсутствие системного подхода в действиях всех ветвей и органов государственной и муниципальной власти.

5. На сегодняшний момент информационная политика российского государства законодательно не оформлена и носит во многом фрагментарный и ситуативный характер. Сама дефиниция «информационная политика» разработана недостаточно глубоко, что отмечается многими учеными и экспертами. В связи с этим в нашей стране продолжается поиск эффективных путей, способов и механизмов реализации отечественных национальных и политических интересов в информационном пространстве. Одновременно в федеральных и региональных органах государственной власти продолжается поиск места и роли информационного пространства в политике. Но пока Интернет, средства массовой информации и пиар-структуры являются скорее своего рода «информационной витриной» деятельности органов государственной власти и местного самоуправления.

6. Во многих государствах мира к началу XXI столетия уже был накоплен немалый опыт функционирования власти в условиях постиндустриального/информационного общества. Государственные органы во многих странах активно формируют специализированные институты (например, электронное правительство, пресс-службы), используют возможности сетевого бизнеса и оказывают все большее количество услуг через информационные сети. Данная тенденция осознана отечественной политической элитой и руководством российского государства, но пока медленно реализуется государственным аппаратом в Российской Федерации. Причиной этого является сложившееся в настоящее время достаточно негативное отношение российского государственного аппарата к любому зарубежному опыту, в т.ч. и к опыту формирования и реализации информационной политики.

7. В настоящее время всё сильнее обостряется конкуренция между различными социально-политическими акторами в информационном пространстве. Результатом конкуренции между государствами и негосударственными структурами стало неизбежное перемещение политики из социальной реальности в информационное пространство, что, в свою очередь, способствует постоянному возрастанию политической роли СМИ и институтов по связям с общественностью. Одновременно всё острее обозначилась проблема соперничества не только реальных государств и социумов, сколько их образов, имиджей, брендов. При этом события августа 2008 года (вооруженный конфликт между Россией и Грузией), случаи с судном «Arctic Sea» и майором А.А. Дымовским, убеждают в том, что давно назрела необходимость формирования эффективных институтов в целях улучшения имиджа нашего государства.

**Степень научной разработанности проблемы.**

Вся изученная профильная литература была предварительно разделена на несколько групп.

Первая группа научных источников, изученных автором, связана с социальными перспективами развития нового информационного общества. Среди ведущих зарубежных специалистов рассмотрены труды Д. Белла, Л. Бриллюэна, И. Валлерстайна, Н. Винера, Э. Гидденса, Дж. Гэлбрейта, П. Дракера, Э. Дюркгейма, М. Кастельса, П.-Ф. Лазарсфельда, Г.-Д. Лассуэл ла, Г. Лебона, Э. Люттвака, А.-Х. Маслоу, Дж. Несбитта, Э. Тоффлера, Л. Туроу, А. Этциони, Ф. Фукуямы, С. Хантингтона, Й. Хейзинга, У. Штанке и др. Определенный вклад в развитие представлений об информационной стадии общественного развития внесли отечественные ученые, среди которых наиболее значимых результатов в советский и постсоветский период достигли В.Г. Афанасьев, В.И. Вернадский, Л.Н. Гумилев, В.С. Егоров, А.П. Ершов, И.А. Ильин, Н.Н. Моисеев, А.И. Ракитов, Ю.А. Нисневич, В.Ф. Ницевич, Г.Л. Смолян, Г.Г. Почепцов, А.Д. Урсул, В.Н. Цыгичко, Д.С. Черешкин, И.И. Юзвишин и другие исследователи. Их работы посвящены проблемам становления и развития информационного общества и информационной цивилизации.

Среди современных отечественных авторов наиболее обстоятельно информационно-политическую проблематику и полито-коммуникационные аспекты власти в современном обществе исследовали А.Н. Аверин, М.С. Вершинин, Б.А. Грушин, Э.Д. Дагбаев, Е.Г. Дьякова, Т.С. Илларионова, Е.В. Карасева, В.З. Коган, В.И. Кравченко, Г.С. Мельник,

И.В. Мелюхин,Т.В. Науменко, Ю.А. Твирова, О.В. Титоренко, А.Д. Урсул, И.П. Цапенко, А.В.Шевченко и ряд других. В научных трудах М.С. Вершинина, Э.А. Галумова, Е.Н. Голубковой, В.П. Конецкой, Г.Г. Почепцова, А.И. Соловьева также рассмотрены различные аспекты социальных коммуникаций, предложены достаточно новые методологические подходы их анализа.

Значение Интернета для общества и для политики проанализировано во многих современных работах. На сегодняшний момент таких работ появляется все больше и больше: исследования проводятся в широком спектре науки, от естественно-технического до социально-гуманитарного. Среди исследований такого рода рассмотрены выполненные в контексте «политика-Интернет» труды В.В. Иванова, Е.Ю. Журавлевой, О.Н. Забузова, К.Н. Кеннета, С.Л. Липатова, С.В. Малахова, И.А. Пенькова, Д.Н. Пескова, Ю.Г. Савостицкого, С.Г. Туронка, А.В. Чугунова, А.Н. Шеремета.

Информационная политика как механизм регулирования информационных процессов и отношений рассматриваются в трудах В.А. Анниковой, В.О. Богомолова, О.Н. Забузова, Е.П. Прохорова, Е.В. Карасёвой, А.Г. Киселева, С.С. Комиссарова, С.В. Коновченко, Ю.А. Нисневича, В.Ф. Ницевича, Д.П. Прудникова. В большинстве этих работ осуществлена достаточно плодотворная попытка сформулировать свой собственный взгляд на сущность и социальные функции информационной политики.

В последние годы вышло немало научных трудов, специально посвященных анализу института связи с общественностью. Среди них отмечены труды И.В. Алёшиной, Н.Ю. Балакиревой, А.А. Белова, Э. Бернейза, Е.В. Блажнова, С. Блэка, О.В. Безгодовой, Дж. Брума, С.А. Варакуты, Е. Грюнинга, Э.Б. Жарниковой, А.Б. Зверинцева, Д.И. Игнатьева, С. Катлипа, И.А. Колотий, В.Г. Королько, В.А. Моисеева, Ф. Сейтела, О.Ю. Становововой, Н. Стоуна, Г.Л. Тульчинского, Т. Ханта, А.Н. Чумикова, М.А. Шишкиной и др.

Отдельным блоком в рамках исследования были изучены научные труды, в которых специально рассмотрены проблемы генезиса и развития электронного государства и электронного правительства. Среди них были изучены исследования А.Н. Авдулова, В.А. Алексунина, К. Барроу, Б. Берковича, Т.А. Бурениной, Н. Вулкан, М.М. Вирина, В. Йордона, В.Ж. Келле, Н. Керстинга, М. Китсинга, О.А. Кобелева, М.В. Кузнецова, А.Н. Кулика, А.М. Кулькина, В.А. Лисичкина, К. Макната, Р. Миллера, Б.З. Мильнера, В. Михалски, И.В. Павлова, З.В. Родигиной, В.Н. Садовского, В.И. Сарафанова, Л.В. Сморгунова, Дж.Е. Фонтэйна, Ц. Чжана, Ю. Шибалова, В. Яковец. В большинстве научных трудов этих и многих других авторов рассматриваются проблемы становления информационного общества и трансформации власти, современные проблемы и противоречия электронного государства, электронного правительства и электронной демократии, перевода процесса выборов власти в Интернет и т.д.

При этом диссертантом обращено внимание на наличие теоретических пробелов в определении дефиниции «информационная политика», ее институциональной структуры, а также механизмов ее формирования и реализации. Фактически пока в отечественных научных изысканиях не удалось соединить достаточно глубокий теоретический анализ с практической политикой государства, не удалось предложить целостную концепцию и модель развития государственной информационной политики. Также пока не удалось в отечественном научном дискурсе четко прояснить и описать ведущую роль политической элиты в формировании и реализации в нашей стране информационной политики. Исходя из этого, диссертантом были сформулированы объект, предмет, цели, задачи и гипотеза научного исследования.

**Цель** исследования – выявить истоки, сущность, содержание и особенности информационной политики современных государств и обосновать применение зарубежного опыта к совершенствованию информационной политики российского государства.

**Задачи** исследования:

– сформулировать и обосновать институциональную обусловленность информационного развития общества;

– рассмотреть современные социально-политические трансформации в качестве катализатора генезиса информационной политики;

– осмыслить политическую роль информационного пространства в современном обществе и государственной политике;

– уточнить основные функции и структуру государственной информационной политики в современном обществе и государстве;

– выработать авторское видение содержания и базовых институтов информационной политики;

– систематизировать и осмыслить мировой опыт формирования и реализации государственной информационной политики;

– проанализировать практику реализации концепции электронного государства в обществе сетевого типа;

– рассмотреть связи с общественностью как средство и институт информационной политики;

– проанализировать эффективность использования информационных технологий в государственной информационной политике Российской Федерации;

– сформулировать и раскрыть основные направления и перспективы формирования коммуникативной компетентности современной российской политической элиты и органов государственной власти;

– предложить механизм формирования и реализации государственной информационной политики в Российской Федерации;

– в авторском варианте выработать оптимальный вариант моделирования отечественной государственной информационной политики.

**Объект** исследования – информационная политика современного государства.

**Предмет** исследования – национально-государственная специфика информационной политики государства.

Диссертантом предложена **научная гипотеза**. Ее суть заключается в предположении о том, что обеспечить социально-политическое развитие нашей страны в XXI столетии и занятие Россией достойного места на международной арене будет крайне сложно без качественно иной политики. Принципиально новое качество российской политике могут придать активное использование всеми акторами информационного пространства, вовлечение в дела государства и общества всех социально-политических субъектов, гражданского общества и граждан, расширение в нашей стране негосударственного пространства. Чтобы добиться этой цели, экспертному сообществу и гражданскому обществу еще предстоит выработать программу развития государственной информационной политики, а затем предложить политической элите и органам власти оптимальную работоспособную модель этой политики.

**На защиту** автор выносит следующие положения:

1. Современная информационная политика формируется и реализуется в трех сферах общественной жизни: социальной, информационной и технической. Основной средой для этого вида политики является информационное пространство, которое составляет невидимую, нематериальную часть жизни социума. Основными институтами современного общества демократического (гражданского) выступили: реальная возможность безграничной эксплуатации природы; институт частной собственности; урбанизация; развитая форма демократии; гражданское общество; национальный тип государственности.

2. Снижение роли материального производства и развитие сектора услуг и информации, иной характер человеческой деятельности, изменившиеся типы вовлекаемых в производство ресурсов, а также существующая модификация традиционной социальной структуры – являются социально-политическими трансформациями, детерминирующий изменения информационной политики. Ускорение социального развития постепенно стало сопрягаться с повышением роли технологического фактора, науки и образования,

качественным изменением места теоретического знания и информации в общественном производстве.

3. Политическое значение и роль информационного пространства в современном социуме постоянно объективно возрастает, т.к. это пространство постоянно расширяется, вовлекая в себя все новые и новые субъекты, институты, сети, т.е. структура информационного пространства также постоянно усложняется. По объективным причинам информационное пространство современного общества все в большей степени интересует власть и все в большей степени становится ее объектом. Политическая роль современного информационного пространства изменяется за счет его способности изменять политическую систему и менять власть (Твиттер-технологии, мобильная связь и т.д.).

4. Основное содержание государственной информационной политики в современном социуме составляют несколько взаимосвязанных процессов. Это формирования информационного законодательства и информатизация деятельности власти и общества, повсеместное создание института связей с общественностью, разработка, создание и внедрение в политический и управленческий процессы информационно-коммуникационных технологий. Функциями информационной политики являются: стимулирование информационными средствами гармоничного развития личности, общества и государства, регулирование общественных отношений и взаимоотношений личности, общества и государства со стороны высшей власти информационными средствами, упрощение и облегчение информационных взаимоотношений между личностью, обществом и государством, обеспечение личности, общественности и органов госвласти объективной информацией о состоянии и развитии социума, создание максимальных возможностей для эффективных действий личности, общества и государства в информационном пространстве.

5. Основное содержание информационной политики в Российской Федерации составляют планомерные действия политической элиты, органов государственной власти и общественных организаций по регулированию информационных отношений. Среди таких действий основными являются создание электронного правительства и электронного государства, выработка полноценной системы информационного законодательства, формирование системы институтов по связям с общественностью, создание и интеграция многочисленных корпоративных и социальных сетей, постоянное внедрение в политические и управленческие процессы современных информационно-коммуникативных технологий. Информационная политика в нашей стране далека от завершенности, но в целом она формируется по общим тенденциям и принципам, которые уже сформированы в демократических государствах.

6. Специфика государственной политики в европейских государствах и США неоднозначна. Во всех странах власть осуществляет нормативное регулирование информационных отношений и процессов, государственное регулирование деятельности печатных и электронных СМИ. Во многих странах вещание с самого начала своего возникновения развивалось как общественное и независимое (частные каналы появились сравнительно недавно). Развитие Интернета рассматривается в качестве социально-политического ресурса. Во многих странах в качестве политической поставлена задача создания единого информационного пространства. В прикладную плоскость переведено создание электронного правительства (перевод большинства государственных услуг в электронный вариант), реализуется концепция «Нового государственного менеджмента».

7. Формирование электронного государства осуществляется, в первую очередь, путем реализации концепции электронного правительства. При этом достигаются общие (для власти и общества) цели деятельности государства: укрепляются и расширяются формы сотрудничества между обществом и государством; более эффективно осуществляется экономическое и социальное развитие общества; повышается эффективность реагирования власти на социальные проблемы; уменьшается стоимость услуг населению; развивается кадровый потенциал государственного управления; повышается ответственность

государственных служащих, поощряется их инициатива и повышается прозрачность государственного управления.

8. Структуры по связям с общественностью в настоящее время являются важнейшим механизмом формирования общественного мнения и институтом информационной политики. С помощью основных методов пиара осуществляется своеобразное «связывание» внутреннего и внешнего информационных пространств в единое целое. Если ранее СМИ являлись основным информационным инструментом, то в последние годы эта роль все в большей степени переходит к Интернету, при этом многие СМИ все активнее действуют в Интернет-пространстве. Основная роль в развитии данного процесса, в его корректировке и регулировании принадлежит политической элите.

9. На примере законодательной власти доказана важность использования информационных технологий в политическом процессе. В настоящее время практически все законодательные органы используют в практике своей работы локальные компьютерные сети, на базе которых применяются правовые автоматизированные информационные системы. В целом ряде законодательных органов нашей страны реализованы автоматизированные системы электронного голосования, делопроизводства и документооборота, компьютерной записи и расшифровки стенограмм заседаний. При этом собственные информационные ресурсы в большинстве регионов объединены в информационные системы, обеспечивающие централизованное накопление и хранение документов с возможностью поиска и просмотра информации на рабочих местах пользователей.

10. Среди основных направлений и перспектив формирования коммуникативной компетентности современной российской политической элиты и органов государственной власти в диссертации выделены информатизация деятельности государственного аппарата и процесса подготовки и принятия важнейших социально значимых решений; развитие у политиков и чиновников компьютерной грамотности; компьютеризация экспертного обеспечения подготовки политических решений; повышение статуса информационной работы в государственном аппарате; повышение статуса действий по формированию позитивного имиджа власти и государства; организация связей с общественностью во всех органах государственной и муниципальной власти; повышение качества медиапланирования в органах государственной власти.

11. Механизм формирования и реализации государственной информационной политики в нашей стране только складывается. Основными компонентами этого механизма являются мировоззренческо-ценностный, нормативно-правовой, функционально-деятельностный и институционально-организационный. В настоящее время основным при формировании информационной политики является мировоззренческо-ценностный компонент, как непосредственно связанный с целеполаганием. Без нормативно-правового компонента, скорее всего, информационная политика не будет проводиться постоянно и целенаправленно в связи с отсутствием четких и обязывающих правовых норм. При реализации информационной политики приоритетным является функционально-деятельностный компонент, поскольку только путем той или иной активности различные социально-политические акторы могут реализовать свои многочисленные интересы.

12. Моделировать государственную информационную модель оказалось достаточно сложно. Авторская модель государственной информационной политики позволяет участникам основных социальных коммуникаций ее оптимизировать. Реализация этой модели на практике не позволит кому-либо монополизировать информационное пространство и, значит, обеспечит динамичное развития современного социума. В прикладном плане эта модель может служить реальной помощью в проведении дальнейших научных изысканий (в том числе комплексных научно-исследовательских работ и диссертаций), выполнении грантов и при подготовке доктринальных документов по тематике государственной информационной политики.

**II. Основное содержание диссертации**

**Во введении** дается обоснование актуальности темы исследования, характеризуется состояние ее разработанности в научной литературе, формулируется объект, предмет, гипотеза, цель, задачи, научная новизна и положения, выносимые на защиту.

В 1-й главе «**Постиндустриальное общество как объект информационной политики**» осмыслены причины изменения традиционного капиталистического общества, приведшего во второй половине XX столетия к возникновению информационной политики. Постиндустриальное общество рассмотрено в качестве объекта информационной политики, а современные социально-политические трансформации – в качестве катализатора генезиса информационной политики. Подробно проанализирована политическая роль современного информационного пространства.

В 1-м параграфе «**Институциональная обусловленность информационного развития общества**» отмечено противоречие в изучении современных социумов. Часть исследователей полагает, что большинство стран сближаются между собой, а их институты и наборы правил становятся все более похожими. Другие ученые считают, что страны не сближаются по уровню развития, а наоборот – разрывы между ними фактически возрастают.

Вторая позиция была обоснована Й. Шумпетером, считавшим, что нечто принципиально новое происходит крайне редко, обычно в области технологий. В обществе чаще происходит некоторая перегруппировка в рамках уже имеющейся парадигмы, а то, что мы принимаем за развитие, как правило, является рекомбинацией тех факторов, которые уже имеют место в социальной практике. То есть, собственная идентичность задает жесткие границы развития любой страны. И, однажды выбрав свою т.н. «колею» развития, та или иная страна уже фактически не может ее изменить.

Достаточно резкое изменение траектории общественного развития требует внесения очень серьезных изменений в формальные и неформальные правила и институты. В рамках институционализма приоритет отдается т.н. надконституционным (т.е. неформальным) правилам, которые сильнее формальных. Неформальные правила никогда не меняются скачкообразно, их можно изменить только очень медленно. Формальные же правила, наоборот, меняются только скачками, которые могут резкими (во время революции и в послереволюционный период), когда существенно или даже кардинальным образом меняются даже конституционные правила.

Политические изменения – это появление новых элементов, характеристик политической жизни и политической системы в результате взаимодействия акторов политического процесса. Отдельные политические изменения взаимосвязаны друг с другом и приводят к рождению новых политических институтов. Крупные качественные изменения в политической сфере приводят к политическому развитию.

Любая политическая система, отмечает профессор С.Г. Кордонский, имеет свойство к воспроизводству своей институциональной структуры определенного типа. К примеру, в России при заселении новых территорий постоянно воспроизводилась социальная структура империи, ее уклады, слои, страты и государственные институты. Профессор В.Э. Багдасарян пишет, что еще в XIX веке была замечена устойчивая повторяемость в идеологическом смысле российских государей через одного, а доминанта западнических тенденций в политике одного неизменно сменялась почвенническим поворотом в последующем царствовании.

Эта повторяемость детерминирована типом взаимоотношений между властью и обществом, общественного договора, под которым обычно подразумевают исторически складывающийся тип взаимоотношений между обществом и госвластью. В социумах, где гражданское общество оказалось сильнее, там возникла преимущественно горизонтальная схема общественного договора, т.е. общество просто распространило свое устройство на свои отношения с властью и на отношения предпринимательской деятельности с властью. Там же, где т.н. гражданское общество оказалось слабее, государство распространило свой

принцип иерархии на отношения с экономикой и обществом. Понятно, что как таковой этот договор носил всегда и носит в настоящее время неформальный/неписаный характер.

Еще одна типологизация траектории общественного развития связана с типом цивилизации. Так, исследователи С.Д. Валентей и Л.И. Нестеров из МГУ им. М.В. Ломоносова выделяют два типа цивилизации: общинный и гражданский.

Предпосылкой возникновения общинного типа цивилизации была родоплеменная организация, при которой интересы племени всегда стояли выше интересов индивида. В это время шел постоянный поиск механизмов, позволяющих сочетать интересы зарождающегося «общества» и «интересы» природы. Форму этого сочетания определил важнейший ограничитель, ибо развитие общества могло базироваться лишь на использовании (естественном потреблении) «сделанного» природой. Следствием же названного ограничителя выступили два результата: в целях самосохранения индивиды должны были объединяться в племена, а племена должны были поддерживать оптимальный оптимум взаимоотношений людей с природой.

При переходе же от родоплеменных (характерных для первобытных охотников и собирателей даров природы) отношений к отношениям общинным (свойственным оседлым землевладельцам) ни одна из вышеназванных особенностей не была преодолена. Подчиненное положение человека было закреплено, а поддержание определенного оптимума населения продолжало сохранять свою значимость. При этом институт общины был дополнен институтом семьи, и вместе они породили третий важный институт – этнический тип государственности.

Другой тип цивилизации, названный С.Д. Валентеем и Л.И. Нестеровым гражданским, формируется примерно в XVI столетии на базе территориальных общностей и локальных цивилизаций, исповедовавших отношения, фундамент которых был заложен еще в Древней Греции. Эти общности характеризовались базовыми особенностями:

- Наряду с признанием силы, в социуме постоянно шел поиск способов самоорганизации, при которых развитие бы пошло по пути приспособления природы к потребностям общества и человека посредством ее эксплуатации.
- Для эллинов и их последователей главной ценностью была свобода граждан, реализуемая через систему демократических институтов.
- Развитие локальных цивилизаций эллинов опиралось на институт личной собственности, что способствовало росту значимости в общественном развитии интересов граждан-горожан.

Такие институты, как свобода граждан, личная собственность, демократия не должны были формироваться в рамках материально-экономической базы, которую предлагала аграрная революция. Из этого учеными делается вывод о серьезном противоречии – поскольку т.н. эллинская цивилизация должна была раствориться в массе общинных локальных и региональных цивилизаций.

Однако т.н. эллинская цивилизация устояла, т.к. был найден некий компенсационный механизм, способный в условиях исключительного господства одной линии общественного развития (общинной) обеспечить воспроизводство общественных институтов, интересов и потребностей иной (гражданской) линии развития. Сочетание института личной собственности и рабовладения требовало формирования соответствующих властных структур и системы управления. В результате возник институт демократии, развивавшийся в рамках трехуровневой структуры социальной организации общества: «граждане-негражданерабы».

Итогом же взаимоналожения социокультурной и материально-экономической составляющих цивилизации гражданского типа выступили:

- Реальная возможность безграничной эксплуатации природы.
- Институт частной собственности.
- Урбанизация.
- Развитая форма демократии.

- Гражданское общество.
- Национальный тип государственности.

Последние три института поспособствовали примерно 350 лет назад началу расцвета цивилизации гражданского типа. Именно эти институты стали доминирующими в развитии социумов, но при этом любые проявления этнического самосознания, выходящие за рамки гражданской цивилизации, вызывали контрмеры. Основная причина заключалась в том, что подобные проявления воспринимались как реальная угроза нации, национальной государственности и национальному экономическому интересу.

Диссертант пришел к выводу о том, что только в социумах гражданского типа со временем может появиться потребность в современной информационной политике.

Во 2-м параграфе «**Современные социально-политические трансформации – катализатор генезиса информационной политики**» диссертант пришел к выводу о том, что технократическое общество, начиная примерно с середины XX столетия начало постепенно трансформироваться в т.н. постиндустриальное общество. Его важнейшим методологическим положением стало подразделение всего общественного производства на первичный (сельское хозяйство), вторичный (промышленность) и третичный (сфера услуг) секторы и предположение о грядущем росте доли третичного сектора по сравнению с первичным и вторичным. Фактически, ускорение социального развития постепенно стало сопрягаться с повышением роли технологического фактора, науки и образования, качественным изменением места теоретического знания и информации в общественном производстве.

Однако вопрос адекватного обозначения формирующегося нового социального состояния вызывал в те годы наибольшее количество споров и дискуссий. В рамках первого подхода прослеживалась генерализация суждений о будущем человечества с несколько радикальных позиций. Так появились определения «постбуржуазного общества», «посткапиталистического строя», «постпредпринимательского» и «пострыночного» общества. Приверженцы же другого подхода предпочитали апеллировать к тому или иному из важнейших признаков нового общества. Так практически одновременно Ф. Махлупа и Т. Умесао в США и Японии ввели термин «информационное общество», а французский социолог А. Турен – «программируемое общество». В русле этого подхода наиболее популярными стали понятия, связанные с указанием на новую технологическую и информационную природу современного общества.

В дальнейшем теория информационного общества была развита такими авторами, как М. Порат, Й. Масуда, Т. Стоуньер, Р. Кац и др. В той или иной мере она получила поддержку со стороны тех исследователей, которые акцентировали внимание не столько на прогрессе собственно информационных технологий, сколько на становлении технологического или технотронного общества или же обозначили современный социум, отталкиваясь от возросшей и постоянно возрастающей роли знаний.

Основой новой концепции (постиндустриального общества) служит оценка нового социума как резко отличающегося от господствовавшего на протяжении последних столетий: снижение роли материального производства и развитие сектора услуг и информации, иной характер человеческой деятельности, изменившиеся типы вовлекаемых в производство ресурсов, а также существующая модификация традиционной социальной структуры.

Считается, что наибольший вклад в развитие концепции постиндустриального общества внес американский социолог Д. Белл. Суть его аналитического метода состояла в признании относительной автономности трех основных сфер социальной жизни. Первой из трех выделяемых им «аналитических сфер» становится то, что он называл «социальной структурой». Второй «аналитических сферой» становится политическая организация общества, роль же политических институтов, по мнению Д. Белла, заключается в минимизации противоречий, неизбежно возникающих в ходе функционирования экономического механизма, а также в преодолении конфликтных ситуаций, порождаемых

иными социальными противоречиями. В этой связи он утверждал, что основным политическим вопросом становится легитимность той власти, которая может быть обращена на решение таких проблем. Наконец, третья сфера представляет собой культуру, т.к. она способна принести в общество (причем естественным и ненасильственным образом) стабильность и преемственность, необходимые ему в процессе развития.

Постепенно во многих социумах во второй половине XX столетия стала формироваться новая конфигурация общества с усилившейся ролью политической системы. Эта роль заключается в более рациональным управлении социальным организмом, скоординированном распределением и перераспределения благ и обеспечения максимальной личной свободы индивида. По мере того, как политический фактор играет все более важную роль, вопрос о том, какие социальные слои окажутся способными непосредственно воздействовать на рычаги управления, приобретают основополагающее значение. Именно отдельные корпоративные группы, основанные на статусных признаках, станут, по мнению Д. Белла, основными субъектами политического процесса в постиндустриальном обществе, где политическая жизнь будет иметь в своем основании «нечто большее, чем сумму политических амбиций людей, объединенных по принципу единой сферы общественной деятельности или социальных групп».

В результате основой этой части политической структуры станет, с одной стороны, «директорат», под которым понимается официальная система государственного управления – от администрации президента через систему законодательной и судебной власти до чиновничьей и военной бюрократии. С другой стороны – это партии и общественные объединения, выражающие интересы более или менее широких устойчивых социальных групп, включая разного рода лоббистские организации, которые стремятся в первую очередь к перераспределению материальных благ или возможностей влияния в пользу своих членов.

Важной в постиндустриальном обществе становится группа людей, которая реально способна установить контроль над приобретающей все большее значение политической системой и осуществлять эффективное управление социальными процессами. По сути дела, речь идет о некоем специфическом слое внутри класса профессионалов (то есть, о людях, в которых воплощены наивысшие возможности и которые обладают наиболее совершенными и разносторонними талантами). Этот слой может быть назван «политическими профессионалами», то есть политиками, профессионально занимающимися только политической деятельностью и больше ничем.

Фактически учеными во второй половине XX столетия был поставлен вопрос о появлении меритократии – некой касте «ученых», во все большей степени монополизирующей рычаги влияния на общество. Утверждение меритократического принципа, само по себе вполне естественное для постиндустриального общества, в то же время означает утверждение фактически непреодолимого наследственного неравенства, в основе которого лежит врожденная способность человека субординировать и продуцировать знания и информацию.

В 3-м параграфе **«Политическая роль современного информационного пространства»** установлено, что главными компонентами информационного пространства выступают социальная информация, средства добывания и доставки этой информации до потребителя, а также от потребителя до источника информации. Информационное пространство определено как некая грань пространства социального, в котором общество с помощью социальной информации, а также средств добывания и доставки этой информации координирует движение человеческого бытия с целью достижения определенных целей и задач.

Важнейшее качество информационного пространства состоит в том, что не всякая информация может служить основой его структуры. Речь в данном случае идет только о социальной информации (в отличие от статистической, семантической, комбинаторной и др.), так как именно социальная информация непосредственно связана с вопросом осмысления и интерпретации доставляемых сведений и сообщений, с пониманием того, что в

них заключено. Но даже социальная информация сама по себе может не иметь социального значения, если не будет доведена до какого-либо потребителя.

В содержательном плане информационное пространство – не просто механическая сумма ресурсов и средств их обработки, а еще и определенная конфигурация отношений различных общественных субъектов к данным ресурсам и средствам. Иными словами, вся та информация, которая поступает в информационное пространство – это отражение в нем информации, которая уже имеет место в социальном пространстве. Каждая сфера общественной жизни имеет свое отражение, свой сегмент в информационном пространстве. Важно, что его сегменты не тождественны аналогичным сегментам социального пространства, как не аналогичны (и не совпадают) социальные и информационные процессы.

Подсистемами информационного пространства являются: СМИ, совокупность аудитории читателей и редакционных организаций, а также собственно информационный продукт, который они создают и распространяют. Эффективное функционирование информационного пространства возможно лишь тогда, когда система СМИ является целостной. Целостность будет обеспечена, когда:

– различные социальные силы имеют равные (в рамках закона) возможности доступа к информационному пространству и распространению в обществе своих взглядов;

– СМИ работают на укрепление и расширение информационных связей (национальных, межрегиональных и региональных);

– информационный процесс обеспечивает на постоянной основе широкие возможности приобщения к духовному потенциалу общества любому гражданину, социальной группе, институту государственной власти;

– обеспечивается гарантированная информационная безопасность личности, общества и государства в информационном пространстве.

Для политической науки значительно больший интерес представляет второе обстоятельство, поскольку связь с реальным социальным пространством в большей степени определяет содержание информационного пространства, нежели технические параметры информационных систем. Определяющими для него являются общественные процессы (в том числе, процессы политические), а также интересы акторов, доминирующих в политическом процессе. Информационное пространство в определенной мере самостоятельно по отношению к пространству социальному. Эта самостоятельность проявляется в появлении субъектов/акторов, действующих только в информационном пространстве и имеющих свои основные интересы в нем.

Формирование информационного пространства современного социума начинается с информатизации, основной целью которой является наиболее полное удовлетворение информационных потребностей личности, общества и государства во всех сферах деятельности, улучшение условий жизни населения, повышение эффективности общественного производства, содействие стабилизации социально-политических отношений в государстве на основе внедрения средств вычислительной техники и телекоммуникаций.

Основным механизмом реализации личности в информационном пространстве являются социальные сети (social networking), т.е. веб-порталы, ориентированные на то, чтобы помочь людям открыть себя друг другу без помощи традиционных социальных институтов. Это достигается путем создания сетевых сообществ (общающихся только в Интернете), в рамках которых пользователи могут свободно обмениваться мыслями, формировать дружественные отношения на базе родства интересов. Современные сетевые сообщества также располагают инструментарием, способствующим духовному и профессиональному росту личности.

Тип взаимоотношений в современных социумах все более становится сетевым. Логика сетевых коммуникаций начинает формировать характер всех коммуникационных процессов, в том числе массовых коммуникаций и политических процессов. Развитые коммуникационные услуги позволяют гражданам формировать власть путем их непрямого контакта с ней. Возможность непрямого участия граждан и сформированных ими структур

позволяет легко обратиться к руководству государства и требовать от властных структур учета или реализации своих интересов, независимо от места нахождения граждан и их статуса в общественной/политической иерархии. Так, мобильная связь способствует созданию новых перспективных моделей взаимодействия государства и граждан в информационном пространстве (m-government).

Приведены примеры активности общества и граждан в информа-ционном пространстве: размещение в Интернете видео-писем милиционера майора А.А. Дымовского председателю Правительства России В.В. Путину (по поводу коррупции в отечественных органах внутренних дел). Другой пример, когда житель одной из челябинских деревень нашел в лесу несколько десятков брошенных танков, снял их на мобильный телефон и выложил эту информацию в Интернете. И как результат – отечественному Министерству обороны пришлось оправдываться и объяснять причины этой ситуации. Еще одним ярким примером того, как граждане, даже напрямую не участвуя в политике, могут активно на нее влиять – является снятие скрытой камерой действий работников ГИБДД в Астраханской области (эти съемки также были выложены в Интернете и долго обсуждались в СМИ и Интернете). В результате – через некоторое время президент России был вынужден начать реформу Министерства внутренних дел.

Во 2-й главе «**Теоретико-методологические основы информационной политики в постиндустриальном обществе**» проанализированы теоретические подходы к пониманию сущности информационной политики и выявлены такие ее сущностные параметры, как функции, содержание, структура и базовые институты.

В 1-м параграфе **«Сущность и основные функции информационной политики»** рассмотрены разные теоретико-методологические подходы к определению сущности информационной политики.

В рамках «бессубъектного подхода» не определяется субъектность информационной политики, но зато достаточно широко и глубоко исследуется влияние информационной политики на обширный круг социальных объектов.

Центральной проблемой информационной политики в рамках технико-коммуникационного подхода рассматривается развитие средств коммуникации. При этом прерогатива отдается развитию технической коммуникационной составляющей.

В рамках «государственнического» подхода ряд ученых определяет информационную политику исключительно как прерогативу государства.

В рамках «социального подхода» под информационной политикой понимается совокупность целей и методов по достижению устойчивого развития информационной сферы жизнедеятельности общества и государства или национальных интересов в информационной сфере. То есть, те или иные регулирующие действия только лишь в информационной сфере общественной жизни.

Специалистами, изучающими информационную политику в рамках «специфического» подхода, предлагается считать действия по регулированию информационных отношений и наращиванию информационных ресурсов.

Диссертант полагает, что информационная политика активно проявляется в трех сферах – социальной, информационной и технической и в определенной степени их же и регулирует. Информационная политика в диссертации рассматривается как совокупность целенаправленных мер органов государственной власти, реализуемых в сотрудничестве с другими институтами политической системы, элементами гражданского общества и иными социальными субъектами в целях развития личности, развития и регулирования социума посредством информационных средств, а также развития и регулирования информационной и технической сферы жизнедеятельности общества и государства.

Основными функциями информационной политики, по мнению диссертанта, являются следующие:

- Стимулирование информационными средствами гармоничного развития личности, общества и государства.

- Регулирование общественных отношений информационными средствами.
- Регулирование информационными средствами взаимоотношений личности, общества и государства со стороны высшей власти.
- Упрощение и облегчение информационных взаимоотношений между личностью, обществом и государством.
- Обеспечение личности, общественности и органов государственной власти объективной информацией о состоянии и развитии социума.
- Создание максимальных возможностей для эффективных действий личности, общества и государства в информационном пространстве.

Во 2-м параграфе **«Структура и базовые институты информационной политики»** основным объектом информационной политики рассмотрено общественное мнение. Общественное мнение является как бы связующим звеном между информационным и социальным пространствами. Различные социальные отношения и связи являются вторичными объектами информационной политики.

Под субъектами (акторами) политики понимаются те, кто принимает реальное участие во властном взаимодействии с государством, независимо от степени влияния на принимаемые им решения и характер реализации государственной политики. Каждый из действующих субъектов способен применять специфические способы и методы воздействия на центры принятия политических решений, а, следовательно, обладает и собственными возможностями влияния на власть и относительно самостоятельной ролью в формировании и развитии самых разных политических процессов.

Субъекты информационной политики с большой долей условности разделены на два вида. К первому виду отнесены субъекты, непосредственно участвующие в политической жизни общества. Этот вид включает три подвида, разделяемые по степени их влияния на процессы выработки и реализации информационной политики. Ко второму виду субъектов отнесены субъекты, принимающие опосредованное участие в политике.

Первый вид субъектов информационной политики:

– Государство и его органы, политические партии, общественно-политические организации и движения.

– Оппозиционные политические партии, лоббистские структуры, транснациональные корпорации (ТНК).

– Средства массовой информации.

– Незаконные (неформальные) организации, которые не являются легальными субъектами политики, но могут оказывать на нее влияние (террористические и экстремистские организации, бандформирования).

Второй вид субъектов информационной политики – это крупные социальные группы и общности, различные группы интересов. То есть, в качестве субъектов информационной политики могут быть рассмотрены любые политические и социальные органы, институты, лидеры, которые активно участвуют в социально-политической жизни и при этом также активно используют информационные средства.

Отмечена важная тенденция развития современного общества, стремящегося стать информационным. Тенденция заключается в том, что информационная политика не может быть лишь исключительно прерогативой государства (в информационном обществе происходит так называемое «разгосударствление политики). Все более активными участниками информационной политики (за счет активности в информационном пространстве) становятся общественно-политические объединения, политические партии, институты гражданского общества, структуры масс-медиа и те, кто за ними стоит, НКО, национальные и наднациональные органы. Происходит как бы размывание основного субъекта (в информационном пространстве этот процесс идет намного быстрее, по сравнению с пространством социальным).

Институциональную структуру государственной информационной политики составляют организации, формирующие ее содержание и цели, а затем реализующие их в

информационном пространстве. К ним относятся: управляющие и координирующие структуры высшей власти; аналитические структуры (представляющие центры ситуационного анализа при различных правительственных ведомствах, в регионах или важнейших структурах власти); базы и банки данных (включая национальные библиотеки); центры защиты информации; центры разработки стандартов информационных контактов (для адаптации к мировому политическому пространству); пиар-службы при государственных органах и соответствующие научно-исследовательские структуры.

Нельзя ставить знак равенства между политическими институтами и институтами информационной политики. Не все социальные (и политические тоже) институты предназначены для функционирования в информационном пространстве. В последнее время появились институты, которые создаются исключительно для действий в этом пространстве (электронные СМИ и пиар-структуры). Следовательно, не все существующие в России социальные институты в одинаковой степени участвуют в выработке и реализации информационной политики. Поэтому институты информационной политики разделены на основные и специализированные.

К основным институтам отнесены Президент, законодательные, исполнительные и судебные органы государственной власти, политические партии, движения и объединения граждан.

В качестве специализированных в диссертации выделены институты, которые создаются только для обеспечения эффективных действий других акторов и социальных институтов в информационном пространстве. В идеале эти институты не должны иметь собственных интересов в социальном пространстве, а их главной задачей является организация постоянной и эффективной коммуникации между различными социальными группами и социально-политическими акторами, формирование того или иного состояния общественного мнения, подготовка и проведение общественных кампаний и др. К ним отнесены государственные и негосударственные средства массовой информации (в первую очередь, электронные) и институт связей с общественностью.

В 3-й главе **«Основное содержание информационной политики в современном государстве»** диссертант обратился к зарубежному опыту государственной информационной политики, а затем рассмотрел ее содержание, предполагая его универсальность для современных стран.

В 1-м параграфе «**Специфика государственной информационной политики в европейских странах и США»** проведен анализ исследований мирового опыта формирования и реализации государственной информационной политики. Выявилась интересная исследовательская картина. Во-первых, таких исследований оказалось не слишком много. Во-вторых, круг этих изысканий свелся к нескольким диссертационным исследованиям по философии, политологии и истории. В-третьих, эти работы можно разделить на несколько видов:

а) работы с анализом реализация информационной политики одного государства по отношению к одному или нескольким государствам;

б) исследования с институциональным анализом механизма формирования информационной политики в зарубежных странах;

в) работы с анализом создания и функционирования т.н. электронного правительства (e-government).

Среди основных направлений реализации государственной информационной политики в зарубежных странах (США, Франция, ФРГ, Австрия, Великобритания) для анализа выделены:

– государственное регулирование деятельности электронных СМИ. Во многих странах вещание с самого начала своего возникновения развивалось как общественное и независимое (но частные каналы появились сравнительно недавно);

– развитие Интернета как социально-политического ресурса;

– нормативное регулирование информационных отношений и процессов;

– создание единого информационного пространства;

– создание электронного правительства (перевод большинства государственных услуг в электронный вариант);

– реализация концепции «Нового государственного менеджмента».

Сделан вывод о том, что в большинстве стран мира информационное пространство является объектом регулирования со стороны политических акторов и органов государственной власти. Наибольшим вниманием во многих странах в настоящее время пользуется Интернет, теле- и аудиовизуальные системы. Традиционные печатные СМИ также не остаются вне политического влияния и контроля со стороны власти и общества. Тенденции и механизмы, присущие информационной политике в развитых странах Запада и США, со временем проявят себя и в нашей стране. Поэтому для любого исследователя-политолога важно изучать зарубежный опыт с целью его последующего применения в России.

Во 2-м параграфе «**Практика реализации концепции электронного государства в обществе сетевого типа»** электронное государство рассматривается как синоним государства XXI столетия, способного обеспечить более устойчивое социально-экономическое развития в условиях неопределенности и повышенных рисков глобализации. Теоретически такое государство способствует восстановлению доверия граждан (если оно по каким-либо причинам было утеряно) к институтам государственной власти и придает новый импульс развитию демократии в информационном (т.е. открытом) обществе. Поэтому созданием электронного государства в настоящее время власть и общественность занимаются в большинстве государств мира.

Одним из основных направлений формирования электронного государства является реализация концепции электронного правительства. При этом достигаются общие (для власти и общества) цели деятельности государства:

- укрепляются и расширяются формы сотрудничества между обществом и государством;
- более эффективно осуществляется экономическое и социальное развитие общества;
- повышается эффективность реагирования власти на социальные проблемы;
- уменьшается стоимость услуг населению;
- развивается кадровый потенциал государственного управления;
- повышается ответственность государственных служащих, поощряется их инициатива и повышается прозрачность госуправления.

Концепция электронного правительства развивается за счет «размещения правительства в сети Интернет», то есть за счет увеличения степени публичности действий органов госвласти. Однако в последние годы многие специалисты отмечают: трансформация публичной политики в начале XXI в. уже сдерживается сложившимися традициями электронного правительства, в котором значительное внимание уделяется качеству услуг и контролю за информацией о деятельности органов государственной власти.

Если в традиционном обществе власть осуществляется в основном правительствами, бюрократией и парламентами (традиционными политическими институтами), то в информационном обществе в публичную власть все больше включаются такие формы, как комиссии, форумы, большие демократически организованные группы. При этом, в информационном обществе информация об управленческих действиях власти становится распределенной и открытой, а информационные процессы, связанные с интерфейсами и протоколами, становятся сетевыми, включают сетевые форумы и систему образования.

В контексте совместной ответственности, а также в рамках понимания социума как сложной самоуправляющейся и самоорганизующейся системы можно понять суть современного информационного общества и способов управления им. В любом обществе и структурах власти люди и их команды постоянно объединяются в подвижные, эволюционирующие структуры, которые зачастую называют сетью сообществ. Именно таким образом формируется социальная ткань иного качества, которая представляет собой

неформальные, взаимодействующие между собой центры самоуправления, демократического принятия решений и сотрудничества. Эти сети существуют в контексте разделяемых ценностей и ориентированы на достижение согласованных общими усилиями целей.

Сети определяют необходимость возникновения объединений, построенных по принципу конфедерации, коалиции, альянса. В сетевых системах нет верхнего и нижнего уровней, деления на уровни, а есть только взаимодействующие узловые пункты ответственности, центры творческого роста, центры действия и энергетические, информационные, коммуникационные меридианы, а также меридианы, отображающие рост потенциала. Сети – это колеблющиеся, живые, развивающиеся коалиции, основным предназначением которых будет решение проблем, производство продукта, обслуживание потребителей, стимуляция личного развития и рост потенциала команды в целом.

Фактически социальные сети возникли с появлением Интернета, который имеет немало преимуществ по сравнению с другими каналами официальной информации о деятельности государства. Он является наиболее удобным и наименее затратным информационным каналом. Присутствие государственных органов в Интернете не только возлагает на них юридическую ответственность за соответствие нормативным актам размещенной на их официальных сайтах информации о деятельности, но и вынуждает их становиться более ответственными по отношению к гражданам, повышает социальную защищенность последних и стимулирует их политическую вовлеченность.

В 3-м параграфе **«Связи с общественностью как средство и институт информационной политики»** институт связей с общественностью рассмотрен в качестве средства органов государственной власти, способного продуцировать новую информацию. Подробно рассмотрены различия связей с общественностью и пропаганды. Их сущностным отличием является следующее: пиар всегда существует в сфере публичной политики, для пропаганды же публичность политического процесса совсем не обязательна.

Достаточно подробно рассмотрена реализация Федеральной целевой программы (ФЦП) «Электронная Россия (2002-2010 годы)». Установлено, что:

- Количество пользователей персональным компьютером в России выросло к 2010 более чем в 10 раз.
- Была расширена законодательная база. Так, в 2005 году принят ФЗ № 94 «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд», а в 2006 году – ФЗ№ 19 «О внесении изменений в некоторые законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов РФ в связи с принятием Федерального закона «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».
- Объем рынка информационных услуг и программного обеспечения возрос в России к 2010 году в 6 раз.
- Количество сайтов и других информационных ресурсов органов государственной власти выросло многократно.

В диссертации подробно проанализировано структура и содержание:

- официального сайта Президента России www.kremlin.ru;
- официального сайта Государственной Думы Федерального Собрания Российской Федерации www.duma.gov.ru;
- официального сайта Совета Федерации Федерального Собрания Российской Федерации www.council.gov.ru;

Подчеркнуто, что сайты Государственной Думы и Совета Федерации предусматривают возможность интерактивного общения с гражданами. Так, на сайте Госдумы презентуется Отдел по работе с обращениями граждан Управления по связям с общественностью и взаимодействию со СМИ, а также указан адрес электронной почты Государственной Думы: stateduma@duma.gov.ru.

Более подробно структура и деятельность Управление по связям с общественностью и взаимодействию со СМИ Аппарата Государственной Думы. Именно это Управление является основной пиар-структурой Государственной Думы Российской Федерации. Аналогичные пиар-органы действуют и в большинстве органов законодательной и исполнительной власти в нашей стране.

Само существование системы связей с общественностью возможно лишь при наличии определенных условий. Главными из них являются: высокий уровень развития гражданского общества, наличие основных гражданских прав и свобод, а также политических институтов, способных влиять не только на общественное мнение, но и на действия любых агентов (органов госвласти, предпринимательских структур, кандидатов на выборах и т.д.), стремящихся управлять этим мнением в своих интересах. К подобным институтам относятся политические партии, общественные объединения, профсоюзы, независимые СМИ, поскольку именно они призваны довести (скорее всего, через собственные информационные ресурсы) до сведения граждан все попытки намеренного сокрытия либо искажения социально важной информации.

В органах государственной и муниципальной власти институты по связям с общественностью выполняют следующие ряд задач:

- установление, поддержание и расширение контактов с гражданами и организациями;
- информирования общественности о существе принимаемых решений;
- изучение общественного мнения, социально-политический мониторинг;
- анализ общественной реакции на действия должностных лиц органов власти;
- прогнозирование социально-политического процесса;
- своевременное обеспечение органов власти прогнозными аналитическими разработками;
- формирование благоприятного имиджа власти и должностных лиц;
- маркетингово-рекламная деятельность;
- информирование средств массовой информации.

Структуры по связям с общественностью в настоящее время являются важнейшим механизмом формирования общественного мнения и институтом информационной политики. С помощью основных методов пиара осуществляется своеобразное «связывание» внутреннего и внешнего информационных пространств в единое целое. Если ранее СМИ являлись основным информационным инструментом, то в последние годы эта роль все в большей степени переходит к Интернету, при этом многие СМИ все активнее действуют в Интернет-пространстве. Сделан вывод о том, что основная роль в развитии данного процесса, в его корректировке и регулировании принадлежит политической элите.

В 4-м параграфе «**Использование информационных технологий в информационной политике государства»** рассмотрена точка зрения большинства российских ученых о том, что в настоящее время наиболее слабым звеном законодательной деятельности является несогласованность социальных интересов в рамках правообразующего процесса, отсутствие анализа последствий прогнозирования принятия законопроектов. Законодательная (представительная) власть, являясь одним из важнейших уровней организации публичной власти, обеспечивает устойчивость и демократический характер всей системы властных институтов. Поэтому сбои и проблемы в работе ее органов негативным образом сказываются на состоянии всего общества.

В настоящее время практически все законодательные органы используют в практике своей работы локальные компьютерные сети, на базе которых применяются правовые автоматизированные информационные системы типа «КонсультантПлюс», «Гарант», «Кодекс», «Система» и другие. В целом ряде законодательных органов нашей страны уже реализованы автоматизированные системы электронного голосования, делопроизводства и документооборота, компьютерной записи и расшифровки стенограмм заседаний. При этом собственные информационные ресурсы в большинстве регионов объединены в

информационные системы, обеспечивающие централизованное накопление и хранение документов с возможностью поиска и просмотра информации на рабочих местах пользователей.

В диссертации представлена и более подробно рассмотрена схема организации и функционирования Фонда электронных информационных ресурсов Государственной Думы РФ.

В настоящее время достаточно серьезно отработана технологическая поддержка взаимодействия законодательных органов субъектов РФ между собой и с федеральными органами законодательной власти в рамках единых интрасетей. Это взаимодействие может осуществляться как в целях информационного обеспечения, так и для непосредственного ввода необходимых данных в определенные технологические системы, например, в АСОЗД Государственной Думы. Подобное взаимодействие обеспечено в объединенной интрасети Государственной Думы и Совета Федерации, имеющей связь с сетями мэрии Москвы, Центральной избирательной комиссии и ряда федеральных ведомств.

Информационным обеспечением в Государственной Думе РФ занимаются Управление документационного и информационного обеспечения, Управление библиотечных фондов (ПБ), Управление по связям с общественностью и СМИ, Правовое управление, Управление государственной службы и кадров. Используемые ими информационные ресурсы обычно подразделяются на внутренние и внешние.

К внешним электронным информационным ресурсам относится информация от высших федеральных органов государственной власти РФ, государственной власти субъектов РФ, федеральных министерств и ведомств, правовая, аналитическая информация и информация российских и зарубежных СМИ. Создание информационно-телекоммуникативной инфраструктуры такого взаимодействия для законодательных органов субъектов Российской Федерации предусмотрено 49-м пунктом Федеральной целевой программы «Электронная Россия».

В диссертации подробно рассмотрена практика реализация в нашей стране Федерального закона «Об электронной цифровой подписи». Обмен электронными документами осуществляется в рамках систем электронного управления документами (СЭУД), эксплуатируемых в Государственной Думе:

- СЭУД «Система автоматизированного делопроизводства и документооборота (САДД)»;
- СЭУД «Электронная почта»;
- СЭУД «Автоматизированная система обеспечения законодательной деятельности (АСОЗД)».

В 4-й главе **«Перспективные направления оптимизации государственной информационной политики в Российской Федерации»** предлагаются варианты формирования коммуникативной компетентности элиты и государственной власти, предложен авторский вариант механизма формирования и реализации информационной политики и перспективная модель деятельности общества и власти в нашей стране по оптимизации этого вида политики.

В 1-м параграфе «**Основные направления и перспективы формирования коммуникативной компетентности современной российской политической элиты и органов государственной власти»** диссертант пришел к выводу о важности наличия у политической элиты и в органах госвласти двух важных качеств. А именно: 1) понимание важности выстраивания современных и эффективных коммуникаций между элитой, с одной стороны, и общественностью и гражданами – с другой (т.е. стратегического видения); 2) политической воли на то, чтобы своевременно и рационально выстроить эти коммуникации. Если два этих базовых качества присутствуют у политической элиты страны, то она способна эффективно развивать политическую коммуникацию в стране, и будет адекватна информационному состоянию современного общества.

Диссертант считает, что пока высшей власти и госаппарату не станет выгодно и полезно быть информационно компетентными, они таковыми не станут. Ключевая проблема информационной компетентности политической элиты заключается в том, что ни для российского общества, ни для отечественной государственной власти информационная компетентность пока еще не стали первоочередной потребностью. В этом случае такая компетентность должна быть обязательно присуща управленческому аппарату, для которого «информационная работа должна рассматриваться как особая форма государственного управления».

Распределение политических ролей в информационном обществе выглядит следующим образом: политическая элита определяет самые общие параметры информационного процесса и те ресурсы, которые она готова для этого выделить, а непосредственно управляет информационным процессом госаппарат (а если еще точнее, то его структуры по связям с общественностью, пресс-службы и т.д.) и специализированные структуры в бизнес-корпорациях в основном через СМИ.

Сформулированы основные направления формирования коммуникативной компетентности современной российской политической элиты и органов государственной власти:

- Формирование социальной ответственности специалистов в области информационной работы и осознание ими того, что они всегда действует от имени государства (или бизнес-корпорации).
- Путем анализа постоянное выявление потребностей, целей и возможностей приоритетных групп отечественной и зарубежной общественности для воздействия со стороны государства.
- Систематическое планирование в рамках выбранной политической коммуникации необходимых информационных мероприятий и своевременное их проведение.
- Постоянное отслеживание и оценка проделанной работы, своевременное внесение соответствующих корректив в собственные планы.
- Уделение особого внимания СМИ с целью выхода на каждую целевую аудиторию общественности и органов государственной власти для наиболее эффективного распространения сообщений.
- Подготовка и регулярное проведение информационных рекламных маркетинговых кампаний.
- Постоянное формирование властью позитивного для себя общественного мнения.
- Постоянная информатизация и компьютеризация государственного аппарата.
- Формирование и постоянное обучение эффективных структур по связям с общественностью во всех органах государственной власти.

В целом диссертант полагает, что от политической элиты и руководства государства зависит формирование в нашей стране информационного общества.

Во 2-м параграфе «**Механизм формирования и реализации государственной информационной политики в Российской Федерации»** данный механизм рассмотрен через такие компоненты, как мировоззренческо-ценностный, нормативно-правовой, институционально-организационный, функционально-деятельностный.

Мировоззренческо-ценностный компонент этого механизма включает мировоззренческую и ценностную составляющие. Различные политические акторы по-разному осмысливают процессы в информационном пространстве и затем их используют и действуют, а значит – принимают и реализуют различные решения, влияющие на социум через информационное пространство. Мировоззрение как бы «переваривает» противоречащие друг другу факты, понятия, оценки и формирует новое знание в виде решения. Т.е. роль мировоззрения заключается в формулировании многочисленных политических представлений и оценок в информационном пространстве как специфической

части объективной реальности. Эти представления и оценки являются в значительной степени основой для последующей выработки и реализации решений в информационном пространстве.

Мировоззренческо-ценностный компонент формирования и реализации информационной политики выступает тем средством, которое обеспечивает познание, понимание и восприятие различными субъектами социально-политического действия политической реальности, которая проявляется/отражается в информационном пространстве и, соответственно, оказывает затем влияние на авторов, органы власти, общественность и граждан – то есть, на социум в целом.

Второй компонент государственной информационной политики – нормативно-правовой. В его рамках рассмотрено содержание Всеобщей декларации прав человека, Хартии глобального информационного общества, Конвенции о преступности в сфере компьютерной информации, Конвенции «Об информационном и правовом сотрудничестве, касающемся «информационных общественных услуг», Федерального Закона РФ «Об информации, информационных технологиях и о защите информации». Сделан вывод о том, что без постоянного совершенствования информационного законодательства невозможна единая и эффективная государственная информационная политика.

Третьим компонентом государственной информационной политики является институционально-организационный компонент. В информационном пространстве деятельность государства сводится к интегрированному волеизъявлению большинства субъектов политики и иных социальных субъектов, заинтересованных в реализации в информационном пространстве собственных интересов. Кроме того, органы государственной власти устанавливают ясные и понятные другим участникам «правила игры» и следят за их обязательным выполнением.

Если власть действительно заинтересована в адекватном представлении своих интересов в обществе, то одной из главнейших задач стоящих перед властью стоит назвать создание и организацию функционирования специализированных институтов. Эти институты должны представлять и реализовывать интересы власти в информационном пространстве. Основными каналами воздействия власти на информационное пространство сегодня стали связи с общественностью и средства массовой информации (электронные, печатные и интернет-СМИ).

Функционально-деятельностный компонент государственной информационной политики показывает степень активности различных субъектов в информационном пространстве. Это та часть механизма, которая приводит его в движение, придает остальным компонентам динамику. Его рассмотрение осуществляется путем анализа принципов информационной деятельности, процесса выработки, принятия и выполнения решений в сфере информационной политики. Этот компонент включает:

- Системы т.н. мобильного правительства (m-government), электронного правительства (e-government) являются ничем иным, как практической реализацией информационной политики.
- Информатизация всех социально значимых проектов в России.
- Вовлечение России в глобальное информационное общество и стремление занять там конкурентоспособные позиции.
- Постоянное внедрение в деятельность органов власти ИКТ.

Функционально-деятельностный компонент государственной информационной политики представлен в виде таблицы/матрицы.

**Матрица для анализа функционально-деятельностного компонента информационной политики**

| Основные модули коммуникации | Структурные составляющие информационной политики | | | |
|---|---|---|---|---|
| | Информационно-техническая | Информационно-правовая | Информационно-политическая | Информационно-экономическая |
| Государство–граждане, общество | | | | |

| | | | | |
|---|---|---|---|---|
| Государство–бизнес | | | | |
| Государство–СМИ | | | | |
| Государство–государство | | | | |

В 3-м параграфе **«Моделирование отечественной государственной информационной политики»** диссертант предложил свой метод моделирования этого вида политики. Для этого диссертант заполнил выделенную в предыдущем параграфе матрицу для анализа функционально-деятельностного компонента информационной политики.

Так, в информационно-технической составляющей коммуникации государства с гражданами и обществом в рамках информационной политики выделены несколько очевидных шагов и/или действий, позволяющих оптимизировать этот вид социального взаимодействия (результаты отражены в отдельном приложении). Они кратко перечислены:

- Широкое использование в нашей стране всеми участниками этой коммуникации открытых государственных и негосударственных каналов связи и информации.
- Предоставление физических каналов доступа российских граждан и общества к информации о деятельности отечественных органов государственной власти.
- Создание в нашей стране многочисленных государственных (с государственным участием) информационных сетей.
- Совместное (всеми участниками коммуникации) использование информации и телекоммуникационной государственной структуры.
- Участие отечественных органов государственной власти в многочисленных социальных сетях.
- Уменьшение в нашей стране разрыва между властью с одной стороны и гражданами и обществом – с другой.
- Использование в нашей стране открытых тендеров на производство информационных работ для отечественных органов государственной власти.
- Снижение экономических издержек на развитие государственных каналов связи и информации в нашей стране.
- Создание в нашей стране механизмов уменьшения количества служебной информации (информации ограниченного доступа).
- Формирование в России технической базы единого национального информационного пространства.
- Выработка в отечественных органах государственной и муниципальной власти четкую позицию о сочетании на практике информационной безопасности и информационного развития Российской Федерации. Эта позиция должна быть прозрачной для российских граждан и общества.

Таким образом, при выполнении этого комплекса действий и мероприятий оптимально будет развиваться техническая сторона государственно-общественного взаимодействия в нашей стране и, соответственно, государственная информационная политика. Диссертант не считает, что тем самым он закрыл тему развития технической стороны государственно-общественного взаимодействия в нашей стране. Наоборот, эта тема открыта для научного анализа и научной дискуссии, которая может быть продолжена на основе сформулированных диссертантом предложений.

Также осуществлено моделирование информационно-правовой составляющей коммуникации российского государства с гражданами и обществом в рамках информационной политики. На основе собственных размышлений и с точки зрения здравого смысла диссертант выделил несколько очевидных шагов/действий, позволяющих оптимизировать этот вид социального взаимодействия (результаты отражены в отдельном приложении). Они кратко перечислены:

- Постоянная работа по совершенствованию информационного законодательства в нашей стране. Создание оптимальных правовых условий для развития информационной сферы российского общества.
- Адаптация национального (российского) и международного информационного законодательства, снятие проблем и разрешение противоречий.
- Привлечение к работе по совершенствованию информационного законодательства основные целевые группы российских граждан (молодежь, ветераны, трудящиеся и т.д.).
- Использование в законотворческой деятельности проектного потенциала российского общества и граждан (например, молодежных парламентов, Форума «Селигер» и др.).
- Использование в нашей стране открытых тендеров на производство законопроектных работ (на основании действующего законодательства).
- Создание и поддержка российской властью новых правовых институтов коммуникации между государством с одной стороны и обществом и гражданами – с другой.
- Совершенствование правоприменительной практики отношений отечественной власти с российским обществом и гражданами.
- Создание и совершенствование в нашей стране правовых механизмов уменьшения количества служебной информации (информации ограниченного доступа).
- Формирование в нашей стране правовой культуры взаимоотношений между властью и обществом гражданского типа.
- Формирование в России правовой базы единого национального информационного пространства, в котором одной из ведущих мест займут общественные организации и граждане.

Таким образом, при выполнении комплекса предложенных диссертантом мероприятий и действий оптимально будет развиваться техническая сторона государственно-общественного взаимодействия в нашей стране и, соответственно, государственная информационная политика в целом. Диссертант не считает закрытой тему развития правовой стороны государственно-общественного взаимодействия в нашей стране.

Аналогичным образом заполнена вся матрица государственной информационной политики, и результаты отражены в 16 специальных приложениях.

**В заключении** формулируются теоретические и практические выводы, предназначенные для дальнейшего изменения социальной роли государственной информационной политики в российском обществе. Их реализация будет способствовать дальнейшему развитию в нашей стране информационного общества и формирования экономики знаний, правого государства и эффективного гражданского общества.

**Источник:** http://www.dissers.ru/avtoreferati-doktorskih-dissertatsii/politika/5/ (14.10.2011)

*ВЛАДИМИР БЕТЕЛИН*
*ВЛАДИМИР ГАЛАТЕНКО*

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РОССИИ: ОПЫТ СОСТАВЛЕНИЯ КАРТЫ

## Введение

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю — национальном, отраслевом, корпоративном или персональном. Для иллюстрации этого положения ограничимся одним примером.

Согласно распоряжению президента США Клинтона (15 июля 1996 года, номер 13010) была создана Комиссия по защите критически важной инфраструктуры как от физических угроз, так и от атак, проводимых с помощью информационного оружия. В начале октября 1997 года, при завершении подготовки доклада президенту, Роберт Марш, глава вышеупомянутой комиссии, заявил, что в настоящее время ни правительство, ни частный сектор не располагают средствами защиты от компьютерных атак, способных вывести из строя коммуникационные сети и сети энергоснабжения.

На наш взгляд, нет оснований предполагать, что Россия обладает большей защищенностью.

В данной работе мы попытаемся составить карту, характеризующую состояние основных аспектов информационной безопасности в России. Нас будут интересовать как уже освоенные области, так и "белые пятна", незаслуженно обойденные вниманием.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать ее специфику, состоящую в том, что информационная безопасность есть составная часть информационных технологий — области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, регламенты, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие жить в темпе технического прогресса.

## Основные определения

Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Из этого довольно очевидного положения можно вывести два важных для нас следствия:

- Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты.
- Информационная безопасность не сводится исключительно к защите информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести материальные и/или моральные убытки) не только от несанкционированного доступа к информации, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственно защита информации стоит по важности отнюдь не на первом месте.

## Грани информационной безопасности

Информационная безопасность — многогранная, можно сказать, многомерная область

деятельности, в которой успех может принести только систематический, комплексный подход. В этом разделе мы укажем важнейшие на наш взгляд грани.

Спектр интересов субъектов, связанных с использованием информационных систем, можно подразделить на следующие основные категории:

- доступность (возможность за приемлемое время получить требуемую информационную услугу);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного ознакомления).

Эти категории будут рассмотрены в Разд. *Доступность, целостность, конфиденциальность.*

Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательного (законы, нормативные акты, стандарты и т.п.);
- административного (действия общего характера, предпринимаемые руководством организации);
- процедурного (конкретные меры безопасности, имеющие дело с людьми);
- программно-технического (конкретные технические меры).

Перечисленные уровни мы рассмотрим в Разд. *Законодательный, административный, процедурный, программно-технический уровни.*

Таковы два основных, на наш взгляд, измерения, задающие систему координат в пространстве информационной безопасности. У информационной безопасности есть и другие грани, но, чтобы чрезмерно не усложнять карту, мы оставим ее двумерной.

### Доступность, целостность, конфиденциальность

#### Доступность

Информационные системы создаются (приобретаются) для получения определенных информационных услуг (сервисов). Если по тем или иным причинам получение этих услуг пользователями становится невозможным, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как важнейший элемент информационной безопасности.

Особенно ярко ведущая роль доступности проявляется в разного рода системах управления — производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия — и материальные, и моральные — может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей. Имеются в виду продажа железнодорожных и авиабилетов, банковские услуги и т.п.

Важность доступности как аспекта информационной безопасности находится в разительном противоречии с тем вниманием, которое уделяют данному аспекту потенциально заинтересованные стороны. Если вопросы защиты от несанкционированного доступа (то есть обеспечение конфиденциальности и целостности информации) курирует Гостехкомиссия России, а криптографические средства (что опять-таки связано с обеспечением конфиденциальности и целостности) — ФАПСИ, то доступностью на государственном уровне не занимается пока никто. На законодательном уровне вопросы доступности затрагиваются только в новой редакции Уголовного кодекса (раздел IX — "Преступления против общественной безопасности", глава 28 — "Преступления в сфере компьютерной информации", статья 274 — "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети").

Авторам не известны отечественные аппаратно-программные продукты общего назначения, повышающие доступность систем (равно как и организации, занимающиеся разработкой таких продуктов). Имеющиеся зарубежные решения не везде применимы и весьма дороги, что существенно сужает круг возможных российских покупателей.

**Целостность**

Целостности повезло больше, чем доступности. Как уже отмечалось, различные аспекты целостности курируют ФАПСИ и Гостехкомиссия. Вышеупомянутая глава 28 УК предусматривает наказания за нарушение целостности. Есть отечественные продукты, обеспечивающие или контролирующие целостность.

В то же время, положение дел с целостностью далеко от идеала. Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Практически все нормативные документы и отечественные разработки относятся к статической целостности, хотя динамический аспект не менее важен. Пример области применения средств контроля динамической целостности — анализ потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

**Конфиденциальность**

Конфиденциальность — самый проработанный у нас в стране аспект информационной безопасности. На страже конфиденциальности стоят законы, нормативные акты, многолетний опыт соответствующих служб. Отечественные аппаратно-программные продукты позволяют закрыть практически все потенциальные каналы утечки информации.

К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить полное представление о потенциальных рисках и степени их серьезности. Во-вторых, авторам не известны отечественные аппаратные реализации шифраторов с достаточным быстродействием, что накладывает ограничения на виды и объемы шифруемой информации. Программные разработки охватывают лишь часть распространенных компьютерных платформ.

**Законодательный, административный, процедурный, программно-технический уровни**

**Законодательный уровень**

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Мы будем различать на законодательном уровне две группы мер:

- меры, направленные на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности;
- направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности.

К первой группе следует отнести в первую очередь главу 28 ("Преступления в сфере компьютерной информации") раздела IX новой редакции Уголовного кодекса. Эта глава достаточно полно охватывает основные угрозы информационным системам, однако обеспечение практической реализуемости соответствующих статей пока остается проблематичным.

Закон "Об информации, информатизации и защите информации" можно причислить к этой же группе. Правда, положения этого закона носят весьма общий характер, а основное содержание статей, посвященных информационной безопасности, сводится к необходимости использовать исключительно сертифицированные средства, что, в общем, правильно, но далеко не достаточно.

Насколько можно судить по планам Государственной Думы, готовятся законы "О праве на

информацию", "О коммерческой тайне", "О персональных данных". Это, безусловно, шаги в правильном направлении, так как делается попытка охватить все категории субъектов информационных отношений.

К группе направляющих и координирующих законов и нормативных актов относится целая группа документов, регламентирующих процессы лицензирования и сертификации в области информационной безопасности. Главная роль здесь отведена Федеральному агентству правительственной связи и информации (ФАПСИ) и Государственной технической комиссии (Гостехкомиссии) при Президенте Российской Федерации.

В области информационной безопасности законы реально преломляются и работают через нормативные документы, подготовленные соответствующими ведомствами. В этой связи очень важны Руководящие документы Гостехкомиссии, определяющие требования к классам защищенности средств вычислительной техники и автоматизированных систем. Особенно выделим утвержденный в июле 1997 года Руководящий документ по межсетевым экранам, вводящий в официальную сферу один из самым современных классов защитных средств.

Как уже указывалось, самое важное на законодательном уровне — создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Конечно, законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности. Пока, пожалуй, только Гостехкомиссия России демонстрирует способность динамично развивать нормативную базу.

В современном мире глобальных сетей нормативно-правовая база должна быть согласована с международной практикой. Мы хотели бы обратить особое внимание на желательность приведения российских стандартов и сертификационных нормативов в соответствие с международным уровнем информационных технологий вообще и информационной безопасности в частности. Есть много причин, по которым это должно быть сделано. Одна из них — необходимость защищенного взаимодействия с зарубежными организациями и зарубежными филиалами российских организаций. Вторая (более существенная) — доминирование аппаратно-программных продуктов зарубежного производства.

На законодательном уровне должен получить реалистичное решение вопрос об отношении к таким изделиям. Здесь необходимо разделить два аспекта: независимость в области информационных технологий и информационную безопасность. Использование зарубежных продуктов в некоторых критически важных системах (в первую очередь военных) в принципе может представлять угрозу национальной безопасности (в том числе информационной), поскольку нельзя исключить вероятности встраивания закладных элементов. В то же время, в подавляющем большинстве случаев потенциальные угрозы информационной безопасности носят исключительно внутренний характер. В таких условиях незаконность использования зарубежных разработок (ввиду сложностей с их сертификацией) при отсутствии отечественных аналогов затрудняет (или вообще делает невозможной) защиту информации без серьезных на то оснований.

Проблема сертификации аппаратно-программных продуктов зарубежного производства действительно является сложной, однако, как показывает опыт европейских стран, она может быть успешно решена. Сложившаяся в Европе система сертификации по требованиям информационной безопасности позволила оценить операционные системы, системы управления базами данных и другие разработки американских компаний. Вхождение России в эту систему и участие российских специалистов в сертификационных испытаниях в состоянии снять имеющееся противоречие между независимостью в области информационных технологий и информационной безопасностью без какого-либо снижения национальной безопасности.

Главное же, чего, на наш взгляд, не хватает современному российскому законодательству (и что можно почерпнуть из зарубежного опыта), это позитивной (не карательной)

направленности. Информационная безопасность — это новая область деятельности, здесь важно научить, разъяснить, помочь, а не запретить и наказать. Общество должно осознать важность данной проблематики, понять основные пути решения соответствующих задач, должны быть скоординированы научные, учебные и производственные планы. Государство может сделать это оптимальным образом. Здесь не нужно больших материальных затрат, требуются интеллектуальные вложения.

Пример позитивного законодательства — Британский стандарт BS 7799:1995, описывающий основные положения политики безопасности (в следующем разделе мы разъясним этот термин). Более 60% крупных организаций используют этот стандарт в своей практике, хотя закон, строго говоря, этого не требует. Еще один пример — Computer Security Act (США), возлагающий на конкретные государственные структуры ответственность за методическую поддержку работ в области информационной безопасности. Со времени вступления этого закона в силу (1988 год) действительно было разработано много важных и полезных документов.

Подводя итог, можно наметить следующие основные направления деятельности на законодательном уровне:

- разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;
- ориентация на созидательные, а не карательные законы;
- интеграция в мировое правовое пространство;
- учет современного состояния информационных технологий.

**Административный уровень**

Основой мер административного уровня, то есть мер, предпринимаемых руководством организации, является политика безопасности.

Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

- вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;
- организационный, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности;
- классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;
- штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п.);
- раздел, освещающий вопросы физической защиты;
- управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;
- раздел, описывающий правила разграничения доступа к производственной информации;
- раздел, характеризующий порядок разработки и сопровождения систем;
- раздел, описывающий меры, направленные на обеспечение непрерывной работы организации;

- юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Административный уровень — белое пятно в отечественной практике информационной безопасности. Нет законов, обязывающих организации иметь политику безопасности. Ни одно из ведомств, курирующих информационную безопасность, не предлагает типовых разработок в данной области. Ни одно учебное заведение не готовит специалистов по составлению политики безопасности. Мало кто из руководителей знает, что такое политика безопасности, еще меньшее число организаций такую политику имеют. В то же время, без подобной основы прочие меры информационной безопасности повисают в воздухе, они не могут быть всеобъемлющими, систематическими и эффективными. Например, меры защиты от внешних хакеров и от собственных обиженных сотрудников должны быть совершенно разными, поэтому в первую очередь необходимо определиться, какие угрозы чреваты нанесением наибольшего ущерба. (Отметим в этой связи, что по статистике наибольший ущерб происходит от случайных ошибок персонала, обусловленных неаккуратностью или некомпетентностью, поэтому в первую очередь важны не хитрые технические средства, а меры обучения, тренировка персонала и регламентирование его деятельности.)

Разработка политики безопасности требует учета специфики конкретных организаций. Бессмысленно переносить практику режимных государственных организаций на коммерческие структуры, учебные заведения или персональные компьютерные системы. В этой области целесообразно предложить, во-первых, основные принципы разработки политики безопасности, а, во-вторых, — готовые шаблоны для наиболее важных разновидностей организаций.

Анализ ситуации на административном уровне информационной безопасности еще раз показывает важность созидательного, а не карательного законодательства. Можно потребовать от руководителей наличия политики безопасности (и в перспективе это правильно), но сначала нужно разъяснить, научить, показать, для чего она нужна и как ее разрабатывать.

**Процедурный уровень**

К процедурному уровню относятся меры безопасности, реализуемые людьми. В отечественных организациях накоплен богатый опыт составления и реализации процедурных (организационных) мер, однако проблема состоит в том, что они пришли из докомпьютерного прошлого, и поэтому нуждаются в существенном пересмотре.

Можно выделить следующие группы процедурных мер, направленных на обеспечение информационной безопасности:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Управление персоналом в контексте информационной безопасности является в России белым пятном. Во-первых, для каждой должности должны существовать квалификационные требования по информационной безопасности. Во-вторых, в должностные инструкции должны входить разделы, касающиеся информационной безопасности. В-третьих, каждого работника нужно научить мерам безопасности теоретически и оттренировать выполнение этих мер практически (и проводить подобные тренировки дважды в год).

Без всякого преувеличения, нужна информационная гражданская оборона. Спокойно, без

нагнетания страстей, нужно разъяснять обществу не только преимущества, но и опасности, вытекающие из использования информационных технологий. Акцент, на наш взгляд, следует делать не на военной или криминальной стороне дела, а на чисто гражданских аспектах, связанных с поддержанием нормального функционирования аппаратного и программного обеспечения, то есть концентрироваться на вопросах доступности и целостности данных.

Разумеется, разделы, касающиеся информационной безопасности, должны стать частью школьных и, тем более, ВУЗовских курсов информатики.

Меры физической защиты, известные с давних времен, нуждаются в доработке в связи с распространением сетевых технологий и миниатюризацией вычислительной техники. Прежде всего, следует защититься от утечки информации по техническим каналам. Этим занимается Гостехкомиссия России.

Поддержание работоспособности — еще одно белое пятно, образовавшееся сравнительно недавно. В эпоху господства больших ЭВМ удалось создать инфраструктуру, способную обеспечить по существу любой наперед заданный уровень работоспособности (доступности) на всем протяжении жизненного цикла информационной системы. Эта инфраструктура включала в себя как технические, так и процедурные регуляторы (обучение персонала и пользователей, проведение работ в соответствии с апробированными регламентами и т.п.). При переходе к персональным компьютерам и технологии клиент/сервер инфраструктура обеспечения доступности во многом оказалась утраченной, однако важность данной проблемы не только не уменьшилась, но, напротив, существенно возросла. Перед государственными и коммерческими организациями стоит задача соединения упорядоченности и регламентированности, присущих миру больших ЭВМ, с открытостью и гибкостью современных систем.

Реагирование на нарушения информационной безопасности — снова белое пятно. Допустим, пользователь или системный администратор понял, что имеет место нарушение. Что он должен делать? Попытаться проследить злоумышленника? Немедленно выключить оборудование? Позвонить в милицию? Проконсультироваться со специалистами ФАПСИ или Гостехкомиссии? Ни одно ведомство, причастное к информационной безопасности, не предложило регламента действий в подобной экстремальной ситуации или своей консультационной помощи. Необходимо организовать национальный центр информационной безопасности, в круг обязанностей которого входило бы, в частности, отслеживание современного состояния этой области знаний, информирование пользователей всех уровней о появлении новых угроз и мерах противодействия, оперативная помощь организациям в случае нарушения их информационной безопасности.

Планирование восстановительных работ и вся проблематика, связанная с восстановлением работоспособности после аварий, также является белым пятном. А ведь ни одна организация от таких нарушений не застрахована. Здесь необходимо отработать действия персонала во время и после аварий, заранее позаботиться об организации резервных производственных площадок, отработать процедуру переноса на эти площадки основных информационных ресурсов, а также процедуру возвращения к нормальному режиму работы. Подчеркнем, что подобный план нужен не только сверхважным военным организациям, но и обычным коммерческим компаниям, если они не хотят понести крупные финансовые потери.

**Программно-технический уровень**

Львиная доля активности в области информационной безопасности приходится на программно-технический уровень. Если иметь в виду зарубежные продукты, здесь существует полный спектр решений. Если ограничиться разработками, имеющими российские сертификаты по требованиям безопасности, картина получается существенно более разреженной.

Согласно современным воззрениям, в рамках информационных систем должны быть доступны по крайней мере следующие механизмы безопасности:

- идентификация и проверка подлинности (аутентификация) пользователей;

- управление доступом;
- протоколирование и аудит;
- криптография;
- (межсетевое) экранирование;
- обеспечение высокой доступности.

Кроме того, информационной системой в целом и механизмами безопасности в особенности необходимо управлять. И управление, и механизмы безопасности должны функционировать в разнородной, распределенной среде, построенной, как правило, в архитектуре клиент/сервер. Это означает, что упомянутые средства должны:

- опираться на общепринятые стандарты;
- быть устойчивыми к сетевым угрозам;
- учитывать специфику отдельных сервисов.

В соответствии с действующим в России порядком, за идентификацию/аутентификацию, управление доступом, протоколирование/аудит отвечает Гостехкомиссия России, за криптографию — ФАПСИ, межсетевое экранирование является спорной территорией, доступностью не занимается никто.

На сегодняшний день подавляющее большинство разработок ориентировано на платформы Intel/DOS/Windows. В то же время, наиболее значимая информация концентрируется на иных, серверных платформах. В защите нуждаются не отдельные персональные компьютеры, не только локальные сети на базе таких компьютеров, но, в первую очередь, существенно более продвинутые современные корпоративные системы. Пока для этого почти нет сертифицированных средств.

Рассмотрим типичную государственную организацию, имеющую несколько производственных площадок, на каждой из которых могут находиться критически важные серверы, в доступе к которым нуждаются работники, базирующиеся на других площадках, и мобильные пользователи. В число поддерживаемых информационных сервисов входят файловый и почтовый сервисы, системы управления базами данных (СУБД), Web-сервис и т.д. В локальных сетях и при межсетевом доступе основным является протокол TCP/IP. Схематически информационная система такой организации представлена на Рис. 1.

**Рисунок 1. Информационная система типичной государственной организации.**


Для построения эшелонированной обороны подобной информационной системы необходимы по крайней мере следующие защитные средства программно-технического уровня:

- межсетевые экраны (разграничение межсетевого доступа);
- средства поддержки частных виртуальных сетей (реализация защищенных коммуникаций между производственными площадками по открытым каналам связи);

- средства идентификации/аутентификации, поддерживающие концепцию единого входа в сеть (пользователь один раз доказывает свою подлинность при входе в сеть организации, после чего получает доступ ко всем имеющимся сервисам в соответствии со своими полномочиями);
- средства протоколирования и аудита, отслеживающие активность на всех уровнях — от отдельных приложений до сети организации в целом, оперативно выявляющие подозрительную активность;
- комплекс средств централизованного администрирования информационной системы организации;
- средства защиты, входящие в состав приложений, сервисов и аппаратно-программных платформ.

На момент написания статьи из интересующего нас спектра продуктов были сертифицированы по требованиям безопасности для применения в госорганизациях ряд межсетевых экранов, операционных систем и реляционных СУБД. Даже если включить в этот перечень продукты, сертифицированные ФАПСИ для применения в коммерческих организациях (систему "ШИП", поддерживающую виртуальные частные сети, и средства криптографической защиты семейства "Верба"), большинство рубежей остается без защиты.

Таким образом, на сегодняшний день государственная организация не может получить современную информационную систему, защищенную сертифицированными средствами.

Коммерческие структуры, в отличие от госорганизаций, в определенной степени свободнее в своем выборе защитных средств. Тем не менее, в силу целого ряда обстоятельств (необходимость взаимодействия с госструктурами, расширительная трактовка понятия гостайны — "гостайна по совокупности", необходимость получения лицензии на эксплуатацию криптосредств, ограничения на импорт криптосредств) эта свобода не слишком велика. Практически на все категории субъектов информационных отношений перенесен подход, рассчитанный на госструктуры.

## Заключение

В предыдущих разделах мы описали двумерное пространство информационной безопасности. Представим результаты наших рассмотрений в наглядной форме, расставив оценки (от 0 до 5), показывающие степень освоенности различных областей в соответствии с современными требованиями и действующим законодательством (Таб. 1).

**Таблица 1. Оценка положения дел в информационной безопасности России.**

| | Доступность | Целостность | Конфиденциальность |
|---|---|---|---|
| законодательный уровень | 1 | 2 | 3 |
| административный уровень | 0 | 0 | 1 |
| процедурный уровень | 0 | 1 | 2 |
| программно-технический уровень | 0 | 1 | 2 |

Информационная безопасность в России развивается крайне неравномерно. Есть давно освоенные области (законодательство о лицензировании и сертификации, программно-технические меры обеспечения конфиденциальности и статической целостности), но большая часть областей, в том числе критически важных, остается белым пятном. Даже на освоенных областях пока не удалось достичь соответствия современным требованиям. Все это позволяет оценить ситуацию с информационной безопасностью в России как крайне тяжелую. Позитивные перемены происходят очень медленно, так что общее отставание от современного уровня продолжает накапливаться.

В то же время, при правильной организации дела положение можно кардинально

улучшить в короткие сроки. Объективно все заинтересованные стороны выиграют от проведения комплексного, современного подхода. Необходима, однако, государственная программа самого высокого уровня, координирующая, направляющая и контролирующая ход работ в области информационной безопасности.

**Источник:** http://unix1.jinr.ru/faq_guide/sec/jet/sec_map/article1.1.1998.html (14.10.2011)

# ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**УТВЕРЖДАЮ:**
Президент Российской Федерации В.Путин
9 сентября 2000 г. № Пр-1895

Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Настоящая Доктрина служит основой для:

- формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Настоящая Доктрина развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

## Глава I. Информационная безопасность Российской Федерации

### 1. Национальные интересы Российской Федерации в информационной сфере и их обеспечение

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере 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 информационной сфере 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 информационной сфере заключаются в создании условий для гармоничного развития российской 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 Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере 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.

Для достижения этого требуется:

- повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа Российской Федерации;
- усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации;
- обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;
- обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;
- укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;
- гарантировать свободу массовой информации и запрет цензуры;
- не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;
- обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной

жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Для достижения этого требуется:

- укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;
- интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

Третья составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, 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 информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Для достижения этого требуется:

- развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;
- развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;
- развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;
- обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

В этих целях необходимо:

- повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;

- интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;
- обеспечить защиту сведений, составляющих государственную тайну;
- расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

**2. Виды угроз информационной безопасности Российской Федерации**

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

- принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;
- создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
- неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;

- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
- снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;
- манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
- блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;
- низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

- противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;
- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

- противоправные сбор и использование информации;

- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

**3. Источники угроз информационной безопасности Российской Федерации**

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние. К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

## 4. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению

За последние годы в Российской Федерации реализован комплекс мер по совершенствованию обеспечения ее информационной безопасности.

Начато формирование базы правового обеспечения информационной безопасности. Приняты Закон Российской Федерации “О государственной тайне”, Основы законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах, федеральные законы “Об информации, информатизации и защите информации”, “Об участии в международном информационном обмене”, ряд других законов, развернута работа по созданию механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Осуществлены мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, на предприятиях, в учреждениях и организациях независимо от формы

собственности. Развернуты работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти.

Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют государственная система защиты информации, система защиты государственной тайны, системы лицензирования деятельности в области защиты государственной тайны и системы сертификации средств защиты информации.

Вместе с тем анализ состояния информационной безопасности Российской Федерации показывает, что ее уровень не в полной мере соответствует потребностям общества и государства.

Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение.

Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере приводят к серьезным негативным последствиям. Так, недостаточность нормативного правового регулирования отношений в области реализации возможностей конституционных ограничений свободы массовой информации в интересах защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороноспособности страны и безопасности государства существенно затрудняет поддержание необходимого баланса интересов личности, общества и государства в информационной сфере. Несовершенное нормативное правовое регулирование отношений в области массовой информации затрудняет формирование на территории Российской Федерации конкурентоспособных российских информационных агентств и средств массовой информации.

Необеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.

Закрепленные в Конституции Российской Федерации права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки практически не имеют достаточного правового, организационного и технического обеспечения. Неудовлетворительно организована защита собираемых федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления данных о физических лицах (персональных данных).

Нет четкости при проведении государственной политики в области формирования российского информационного пространства, развития системы массовой информации, организации международного информационного обмена и интеграции информационного пространства России в мировое информационное пространство, что создает условия для вытеснения российских информационных агентств, средств массовой информации с внутреннего информационного рынка и деформации структуры международного информационного обмена.

Недостаточна государственная поддержка деятельности российских информационных агентств по продвижению их продукции на зарубежный информационный рынок.

Ухудшается ситуация с обеспечением сохранности сведений, составляющих государственную тайну.

Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов.

Отставание отечественных информационных технологий вынуждает федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации и органы местного самоуправления при создании информационных систем идти по пути закупок импортной техники и привлечения иностранных фирм, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно-телекоммуникационных систем, интеграцией отечественных информационных систем и международных информационных систем возросли угрозы применения “информационного оружия” против информационной инфраструктуры России. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании. Недостаточное внимание уделяется развитию средств космической разведки и радиоэлектронной борьбы.

Сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательного решения таких задач, как:

- разработка основных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации, а также мероприятий и механизмов, связанных с реализацией этой политики;
- развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Российской Федерации, а также системы противодействия этим угрозам;
- разработка федеральных целевых программ обеспечения информационной безопасности Российской Федерации;
- разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации, а также сертификации этих систем и средств;
- совершенствование нормативной правовой базы обеспечения информационной безопасности Российской Федерации, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации;
- установление ответственности должностных лиц федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности;
- координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, предприятий, учреждений

и организаций независимо от формы собственности в области обеспечения информационной безопасности Российской Федерации;
- развитие научно-практических основ обеспечения информационной безопасности Российской Федерации с учетом современной геополитической ситуации, условий политического и социально-экономического развития России и реальности угроз применения “информационного оружия”;
- разработка и создание механизмов формирования и реализации государственной информационной политики России;
- разработка методов повышения эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;
- обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность, и в первую очередь в области создания специализированной вычислительной техники для образцов вооружения и военной техники;
- разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;
- развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;
- создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;
- расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;
- обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;
- создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

## Глава II. Методы обеспечения информационной безопасности Российской Федерации

### 5. Общие методы обеспечения информационной безопасности Российской Федерации

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации. Наиболее важными направлениями этой деятельности являются:

- внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности Российской Федерации, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась Российская Федерация, и противоречий между федеральными законодательными актами и законодательными актами

субъектов Российской Федерации, а также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности Российской Федерации;

- законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;
- разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;
- уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России;
- законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;
- определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций;
- создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.

Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются:

- создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;
- усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;
- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;
- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;

- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;
- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;
- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;
- формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя:

- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

## 6. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни

Информационная безопасность Российской Федерации является одной из составляющих национальной безопасности Российской Федерации и оказывает влияние на защищенность национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства. Угрозы информационной безопасности Российской Федерации и методы ее обеспечения являются общими для этих сфер.

В каждой из них имеются свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении угроз информационной безопасности Российской Федерации. В каждой сфере жизнедеятельности общества и государства наряду с общими методами обеспечения информационной безопасности Российской Федерации могут использоваться частные методы и формы, обусловленные спецификой факторов, влияющих на состояние информационной безопасности Российской Федерации.

**В сфере экономики.** Обеспечение информационной безопасности Российской Федерации в сфере экономики играет ключевую роль в обеспечении национальной безопасности Российской Федерации.

Воздействию угроз информационной безопасности Российской Федерации в сфере экономики наиболее подвержены:

- система государственной статистики;
- кредитно-финансовая система;
- информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;

- системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;
- системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

Переход к рыночным отношениям в экономике вызвал появление на внутреннем российском рынке товаров и услуг множества отечественных и зарубежных коммерческих структур - производителей и потребителей информации, средств информатизации и защиты информации. Бесконтрольная деятельность этих структур по созданию и защите систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации создает реальную угрозу безопасности России в экономической сфере. Аналогичные угрозы возникают при бесконтрольном привлечении иностранных фирм к созданию подобных систем, поскольку при этом складываются благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации и для контроля за процессами ее передачи и обработки со стороны иностранных спецслужб.

Критическое состояние предприятий национальных отраслей промышленности, разрабатывающих и производящих средства информатизации, телекоммуникации, связи и защиты информации, приводит к широкому использованию соответствующих импортных средств, что создает угрозу возникновения технологической зависимости России от иностранных государств.

Серьезную угрозу для нормального функционирования экономики в целом представляют компьютерные преступления, связанные с проникновением криминальных элементов в компьютерные системы и сети банков и иных кредитных организаций.

Недостаточность нормативной правовой базы, определяющей ответственность хозяйствующих субъектов за недостоверность или сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг, о результатах их хозяйственной деятельности, об инвестициях и тому подобном, препятствует нормальному функционированию хозяйствующих субъектов. В то же время существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну. В системах сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации наиболее опасны противоправное копирование информации и ее искажение вследствие преднамеренных или случайных нарушений технологии работы с информацией, несанкционированного доступа к ней. Это касается и федеральных органов исполнительной власти, занятых формированием и распространением информации о внешнеэкономической деятельности Российской Федерации.

Основными мерами по обеспечению информационной безопасности Российской Федерации в сфере экономики являются:

- организация и осуществление государственного контроля за созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;
- коренная перестройка системы государственной статистической отчетности в целях обеспечения достоверности, полноты и защищенности информации, осуществляемая путем введения строгой юридической ответственности должностных лиц за подготовку первичной информации, организацию контроля за деятельностью этих

лиц и служб обработки и анализа статистической информации, а также путем ограничения коммерциализации такой информации;
- разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;
- разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли, стандартизация этих систем, а также разработка нормативной правовой базы, регламентирующей их использование;
- совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;
- совершенствование методов отбора и подготовки персонала для работы в системах сбора, обработки, хранения и передачи экономической информации.

**В сфере внутренней политики.** Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

- конституционные права и свободы человека и гражданина;
- конституционный строй, национальное согласие, стабильность государственной власти, суверенитет и территориальная целостность Российской Федерации;
- открытые информационные ресурсы федеральных органов исполнительной власти и средств массовой информации.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации:

- нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;
- недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;
- распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;
- деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

Основными мероприятиями в области обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

- создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации;
- активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России.

**В сфере внешней политики.** К наиболее важным объектам обеспечения информационной безопасности Российской Федерации в сфере внешней политики относятся:

- информационные ресурсы федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;
- информационные ресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, на территориях субъектов Российской Федерации;
- информационные ресурсы российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующим внешнюю политику Российской Федерации;
- блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики Российской Федерации, ее мнения по социально значимым событиям российской и международной жизни.

Из внешних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

- информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;
- распространение за рубежом дезинформации о внешней политике Российской Федерации;
- нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;
- попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях.

Из внутренних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

- нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику Российской Федерации, и на подведомственных им предприятиях, в учреждениях и организациях;
- информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности Российской Федерации;
- недостаточная информированность населения о внешнеполитической деятельности Российской Федерации.

Основными мероприятиями по обеспечению информационной безопасности Российской Федерации в сфере внешней политики являются:

- разработка основных направлений государственной политики в области совершенствования информационного обеспечения внешнеполитического курса Российской Федерации;
- разработка и реализация комплекса мер по усилению информационной безопасности информационной инфраструктуры федеральных органов исполнительной власти,

реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;
- создание российским представительствам и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике Российской Федерации;
- совершенствование информационного обеспечения работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом;
- совершенствование информационного обеспечения субъектов Российской Федерации по вопросам внешнеполитической деятельности, которые входят в их компетенцию.

В области науки и техники. Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в области науки и техники являются:

- результаты фундаментальных, поисковых и прикладных научных исследований, потенциально важные для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;
- открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование;
- научно-технические кадры и система их подготовки;
- системы управления сложными исследовательскими комплексами (ядерными реакторами, ускорителями элементарных частиц, плазменными генераторами и другими).

К числу основных внешних угроз информационной безопасности Российской Федерации в области науки и техники следует отнести:

- стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах;
- создание льготных условий на российском рынке для иностранной научно-технической продукции и стремление развитых стран в то же время ограничить развитие научно-технического потенциала России (скупка акций передовых предприятий с их последующим перепрофилированием, сохранение экспортно-импортных ограничений и тому подобное);
- политику западных стран, направленную на дальнейшее разрушение унаследованного от СССР единого научно-технического пространства государств - участников Содружества Независимых Государств за счет переориентации на западные страны их научно-технических связей, а также отдельных, наиболее перспективных научных коллективов;
- активизацию деятельности иностранных государственных и коммерческих предприятий, учреждений и организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб.

К числу основных внутренних угроз информационной безопасности Российской Федерации в области науки и техники следует отнести:

- сохраняющуюся сложную экономическую ситуацию в России, ведущую к резкому снижению финансирования научно-технической деятельности, временному падению престижа научно-технической сферы, утечке за рубеж идей и передовых разработок;

- неспособность предприятий национальных отраслей электронной промышленности производить на базе новейших достижений микроэлектроники, передовых информационных технологий конкурентоспособную наукоемкую продукцию, позволяющую обеспечить достаточный уровень технологической независимости России от зарубежных стран, что приводит к вынужденному широкому использованию импортных программно-аппаратных средств при создании и развитии в России информационной инфраструктуры;
- серьезные проблемы в области патентной защиты результатов научно-технической деятельности российских ученых;
- сложности реализации мероприятий по защите информации, особенно на акционированных предприятиях, в научно-технических учреждениях и организациях.

Реальный путь противодействия угрозам информационной безопасности Российской Федерации в области науки и техники - это совершенствование законодательства Российской Федерации, регулирующего отношения в данной области, и механизмов его реализации. В этих целях государство должно способствовать созданию системы оценки возможного ущерба от реализации угроз наиболее важным объектам обеспечения информационной безопасности Российской Федерации в области науки и техники, включая общественные научные советы и организации независимой экспертизы, вырабатывающие рекомендации для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации по предотвращению противоправного или неэффективного использования интеллектуального потенциала России.

В сфере духовной жизни. Обеспечение информационной безопасности Российской Федерации в сфере духовной жизни имеет целью защиту конституционных прав и свобод человека и гражданина, связанных с развитием, формированием и поведением личности, свободой массового информирования, использования культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни, с сохранением культурного достояния всех народов России, реализацией конституционных ограничений прав и свобод человека и гражданина в интересах сохранения и укрепления нравственных ценностей общества, традиций патриотизма и гуманизма, здоровья граждан, культурного и научного потенциала Российской Федерации, обеспечения обороноспособности и безопасности государства.

К числу основных объектов обеспечения информационной безопасности Российской Федерации в сфере духовной жизни относятся:

- достоинство личности, свобода совести, включая право свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними, свобода мысли и слова (за исключением пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду), а также свобода литературного, художественного, научного, технического и других видов творчества, преподавания;
- свобода массовой информации;
- неприкосновенность частной жизни, личная и семейная тайна;
- русский язык как фактор духовного единения народов многонациональной России, язык межгосударственного общения народов государств-участников Содружества Независимых Государств;
- языки, нравственные ценности и культурное наследие народов и народностей Российской Федерации;
- объекты интеллектуальной собственности.

Наибольшую опасность в сфере духовной жизни представляют следующие угрозы информационной безопасности Российской Федерации:

- деформация системы массового информирования как за счет монополизации средств массовой информации, так и за счет неконтролируемого расширения сектора зарубежных средств массовой информации в отечественном информационном пространстве;
- ухудшение состояния и постепенный упадок объектов российского культурного наследия, включая архивы, музейные фонды, библиотеки, памятники архитектуры, ввиду недостаточного финансирования соответствующих программ и мероприятий;
- возможность нарушения общественной стабильности, нанесение вреда здоровью и жизни граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект;
- использование зарубежными специальными службами средств массовой информации, действующих на территории Российской Федерации, для нанесения ущерба обороноспособности страны и безопасности государства, распространения дезинформации;
- неспособность современного гражданского общества России обеспечить формирование у подрастающего поколения и поддержание в обществе общественно необходимых нравственных ценностей, патриотизма и гражданской ответственности за судьбу страны.

Основными направлениями обеспечения информационной безопасности Российской Федерации в сфере духовной жизни являются:

- развитие в России основ гражданского общества;
- создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры;
- выработка цивилизованных форм и способов общественного контроля за формированием в обществе духовных ценностей, отвечающих национальным интересам страны, воспитанием патриотизма и гражданской ответственности за ее судьбу;
- совершенствование законодательства Российской Федерации, регулирующего отношения в области конституционных ограничений прав и свобод человека и гражданина;
- государственная поддержка мероприятий по сохранению и возрождению культурного наследия народов и народностей Российской Федерации;
- формирование правовых и организационных механизмов обеспечения конституционных прав и свобод граждан, повышения их правовой культуры в интересах противодействия сознательному или непреднамеренному нарушению этих конституционных прав и свобод в сфере духовной жизни;
- разработка действенных организационно-правовых механизмов доступа средств массовой информации и граждан к открытой информации о деятельности федеральных органов государственной власти и общественных объединений, обеспечение достоверности сведений о социально значимых событиях общественной жизни, распространяемых через средства массовой информации;
- разработка специальных правовых и организационных механизмов недопущения противоправных информационно-психологических воздействий на массовое сознание общества, неконтролируемой коммерциализации культуры и науки, а также обеспечивающих сохранение культурных и исторических ценностей народов и народностей Российской Федерации, рациональное использование накопленных обществом информационных ресурсов, составляющих национальное достояние;

- введение запрета на использование эфирного времени в электронных средствах массовой информации для проката программ, пропагандирующих насилие и жестокость, антиобщественное поведение;
- противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

В общегосударственных информационных и телекоммуникационных системах. Основными объектами обеспечения информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

- информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;
- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;
- технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации;
- помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа.

Основными угрозами информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

- деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных и телекоммуникационных систем;
- вынужденное в силу объективного отставания отечественной промышленности использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств;
- нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;
- использование несертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты информации и контроля их эффективности;
- привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности.

Основными направлениями обеспечения информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств;

- исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи;
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;
- обеспечение информационной безопасности при подключении общегосударственных информационных и телекоммуникационных систем к внешним информационным сетям, включая международные;
- обеспечение безопасности конфиденциальной информации при взаимодействии информационных и телекоммуникационных систем различных классов защищенности;
- выявление внедренных на объекты и в технические средства электронных устройств перехвата информации.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- лицензирование деятельности организаций в области защиты информации;
- аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

**В сфере обороны.** К объектам обеспечения информационной безопасности Российской Федерации в сфере обороны относятся:

- информационная инфраструктура центральных органов военного управления и органов военного управления видов Вооруженных Сил Российской Федерации и родов войск, объединений, соединений, воинских частей и организаций, входящих в Вооруженные Силы Российской Федерации, научно-исследовательских учреждений Министерства обороны Российской Федерации;
- информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;
- программно-технические средства автоматизированных и автоматических систем управления войсками и оружием, вооружения и военной техники, оснащенных средствами информатизации;
- информационные ресурсы, системы связи и информационная инфраструктура других войск, воинских формирований и органов.

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности Российской Федерации в сфере обороны, являются:

- все виды разведывательной деятельности зарубежных государств;
- информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети) со стороны вероятных противников;
- диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;
- деятельность иностранных политических, экономических и военных структур, направленная против интересов Российской Федерации в сфере обороны.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях министерства обороны российской федерации, на предприятиях оборонного комплекса;
- преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;
- ненадежное функционирование информационных и телекоммуникационных систем специального назначения;
- возможная информационно-пропагандистская деятельность, подрывающая престиж вооруженных сил российской федерации и их боеготовность;
- нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов;
- нерешенность вопросов социальной защиты военнослужащих и членов их семей.

Перечисленные внутренние угрозы будут представлять особую опасность в условиях обострения военно-политической обстановки.

Главными специфическими направлениями совершенствования системы обеспечения информационной безопасности Российской Федерации в сфере обороны являются:

- систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности в сфере обороны и определение соответствующих практических задач;
- проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления военного назначения и системах связи, имеющих в своем составе элементы вычислительной техники;
- постоянное совершенствование средств защиты информации от несанкционированного доступа, развитие защищенных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;
- совершенствование структуры функциональных органов системы обеспечения информационной безопасности в сфере обороны и координация их взаимодействия;
- совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника;
- подготовка специалистов в области обеспечения информационной безопасности в сфере обороны.

**В правоохранительной и судебной сферах.** К наиболее важным объектам обеспечения информационной безопасности в правоохранительной и судебной сферах относятся:

- информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;
- информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;
- информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).
- Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности в правоохранительной и судебной сферах, являются:
    - разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп, связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел Российской Федерации;
    - деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и использующейся для расследования преступлений;
- недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;
- отсутствие единой методологии сбора, обработки и хранения информации оперативно-разыскного, справочного, криминалистического и статистического характера;
- отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;
- преднамеренные действия, а также ошибки персонала, непосредственно занятого формированием и ведением картотек и автоматизированных банков данных.

Наряду с широко используемыми общими методами и средствами защиты информации применяются также специфические методы и средства обеспечения информационной безопасности в правоохранительной и судебной сферах.

Главными из них являются:

- создание защищенной многоуровневой системы интегрированных банков данных оперативно-разыскного, справочного, криминалистического и статистического характера на базе специализированных информационно-телекоммуникационных систем;
- повышение уровня профессиональной и специальной подготовки пользователей информационных систем.

В условиях чрезвычайных ситуаций. Наиболее уязвимыми объектами обеспечения информационной безопасности Российской Федерации в условиях чрезвычайных ситуаций являются система принятия решений по оперативным действиям (реакциям), связанным с развитием таких ситуаций и ходом ликвидации их последствий, а также система сбора и обработки информации о возможном возникновении чрезвычайных ситуаций.

Особое значение для нормального функционирования указанных объектов имеет обеспечение безопасности информационной инфраструктуры страны при авариях, катастрофах и стихийных бедствиях. Сокрытие, задержка поступления, искажение и разрушение оперативной информации, несанкционированный доступ к ней отдельных лиц или групп лиц могут привести как к человеческим жертвам, так и к возникновению разного рода сложностей при ликвидации последствий чрезвычайной ситуации, связанных с особенностями информационного воздействия в экстремальных условиях: к приведению в движение больших масс людей, испытывающих психический стресс, к быстрому возникновению и распространению среди них паники и беспорядков на основе слухов, ложной или недостоверной информации.

К специфическим для данных условий направлениям обеспечения информационной безопасности относятся:

- разработка эффективной системы мониторинга объектов повышенной опасности, нарушение функционирования которых может привести к возникновению чрезвычайных ситуаций, и прогнозирования чрезвычайных ситуаций;
- совершенствование системы информирования населения об угрозах возникновения чрезвычайных ситуаций, об условиях их возникновения и развития;
- повышение надежности систем обработки и передачи информации, обеспечивающих деятельность федеральных органов исполнительной власти;
- прогнозирование поведения населения под воздействием ложной или недостоверной информации о возможных чрезвычайных ситуациях и выработка мер по оказанию помощи большим массам людей в условиях этих ситуаций;
- разработка специальных мер по защите информационных систем, обеспечивающих управление экологически опасными и экономически важными производствами.

## 7. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности

Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности - 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 Российскую Федерацию.

Особенность международного сотрудничества Российской Федерации в области обеспечения информационной безопасности состоит в том, что оно осуществляется в условиях обострения международной конкуренции за обладание технологическими и информационными ресурсами, за доминирование на рынках сбыта, 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 информационной сфере, нарастанию угрозы агентурного

и оперативно-технического проникновения в Россию иностранных разведок, в том числе с использованием глобальной информационной инфраструктуры.

Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности являются:

- 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 информационного обеспечения мировой торговли, к информации международных 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 Российской Федерации в области обеспечения информационной безопасности особое внимание должно уделяться проблемам взаимодействия с государствами - участниками Содружества Независимых Государств.

Для осуществления этого сотрудничества по указанным основным направлениям необходимо обеспечить активное участие России во всех международных организациях, осуществляющих деятельность в области информационной безопасности, в том числе в сфере стандартизации и сертификации средств информатизации и защиты информации.

## Глава III. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации

### 8. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации

Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих основных принципах:

- соблюдение Конституции Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации;
- открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных

объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;
- правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;
- приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Государство в процессе реализации своих функций по обеспечению информационной безопасности Российской Федерации:

- проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности Российской Федерации, разрабатывает меры по ее обеспечению;
- организует работу законодательных (представительных) и исполнительных органов государственной власти Российской Федерации по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации;
- поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;
- осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;
- проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории Российской Федерации и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;
- способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;
- формулирует и реализует государственную информационную политику России;
- организует разработку федеральной программы обеспечения информационной безопасности Российской Федерации, объединяющей усилия государственных и негосударственных организаций в данной области;
- способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности Российской Федерации.

Это предполагает:

- оценку эффективности применения действующих законодательных и иных нормативных правовых актов в информационной сфере и выработку программы их совершенствования;

- создание организационно-правовых механизмов обеспечения информационной безопасности;
- определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем, и установление их ответственности за соблюдение законодательства Российской Федерации в данной сфере;
- создание системы сбора и анализа данных об источниках угроз информационной безопасности Российской Федерации, а также о последствиях их осуществления;
- разработку нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий;
- разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство Российской Федерации о государственной службе;
- совершенствование системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации.

Правовое обеспечение информационной безопасности Российской Федерации должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере.

Соблюдение принципа законности требует от федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации при решении возникающих в информационной сфере конфликтов неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере.

Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

Разработка механизмов правового обеспечения информационной безопасности Российской Федерации включает в себя мероприятия по информатизации правовой сферы в целом.

В целях выявления и согласования интересов федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и других субъектов отношений в информационной сфере, выработки необходимых решений государство поддерживает формирование общественных советов, комитетов и комиссий с широким представительством общественных объединений и содействует организации их эффективной работы.

**9. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности Российской Федерации**

Первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности Российской Федерации являются:

- разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка концепции правового обеспечения информационной безопасности Российской Федерации;
- разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществления государственной информационной политики;
- принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, повышение правовой культуры и компьютерной грамотности граждан, развитие инфраструктуры единого информационного пространства России, комплексное противодействие угрозам информационной войны, создание безопасных информационных технологий для систем, используемых в процессе реализации жизненно важных функций общества и государства, пресечение компьютерной преступности, создание информационно-телекоммуникационной системы специального назначения в интересах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, обеспечение технологической независимости страны в области создания и эксплуатации информационно-телекоммуникационных систем оборонного назначения;
- развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации;
- гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления, информационных и телекоммуникационных систем общего и специального назначения.

## Глава IV. Организационная основа системы обеспечения информационной безопасности Российской Федерации

### 10. Основные функции системы обеспечения информационной безопасности Российской Федерации

Система обеспечения информационной безопасности Российской Федерации предназначена для реализации государственной политики в данной сфере.

Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

- разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;
- создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;
- определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;
- оценка состояния информационной безопасности Российской Федерации, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;

- координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности Российской Федерации;
- контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности Российской Федерации;
- предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;
- развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;
- организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;
- проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;
- организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;
- защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;
- обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;
- совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации;
- осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Компетенция федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяется федеральными законами, нормативными правовыми актами Президента Российской Федерации и Правительства Российской Федерации.

Функции органов, координирующих деятельность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяются отдельными нормативными правовыми актами Российской Федерации.

## 11. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации

Система обеспечения информационной безопасности Российской Федерации является частью системы обеспечения национальной безопасности страны.

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной

власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются: Президент Российской Федерации, Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с законодательством Российской Федерации участие в решении задач обеспечения информационной безопасности Российской Федерации.

Президент Российской Федерации руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности Российской Федерации; санкционирует действия по обеспечению информационной безопасности Российской Федерации; в соответствии с законодательством Российской Федерации формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной безопасности Российской Федерации; определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения информационной безопасности Российской Федерации, а также меры по реализации настоящей Доктрины.

Палаты Федерального Собрания Российской Федерации на основе Конституции Российской Федерации по представлению Президента Российской Федерации и Правительства Российской Федерации формируют законодательную базу в области обеспечения информационной безопасности Российской Федерации.

Правительство Российской Федерации в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента Российской Федерации Федеральному Собранию приоритетных направлений в области обеспечения информационной безопасности Российской Федерации координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, а также при формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.

Совет Безопасности Российской Федерации проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации, оперативно подготавливает проекты решений Президента Российской Федерации по предотвращению таких угроз, разрабатывает предложения в области обеспечения информационной безопасности Российской Федерации, а также предложения по уточнению отдельных положений настоящей Доктрины, координирует деятельность органов и сил по обеспечению информационной безопасности Российской Федерации, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации решений Президента Российской Федерации в этой области.

Федеральные органы исполнительной власти обеспечивают исполнение законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской

Федерации; в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и представляют их в установленном порядке Президенту Российской Федерации и в Правительство Российской Федерации.

Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности Российской Федерации.

Органы исполнительной власти субъектов Российской Федерации взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности Российской Федерации; вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения информационной безопасности Российской Федерации.

Органы местного самоуправления обеспечивают соблюдение законодательства Российской Федерации в области обеспечения информационной безопасности Российской Федерации.

Органы судебной власти осуществляют правосудие по делам о преступлениях, связанных с посягательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению информационной безопасности Российской Федерации.

В состав системы обеспечения информационной безопасности Российской Федерации могут входить подсистемы (системы), ориентированные на решение локальных задач в данной сфере.

Реализация первоочередных мероприятий по обеспечению информационной безопасности Российской Федерации, перечисленных в настоящей Доктрине, предполагает разработку соответствующей федеральной программы. Конкретизация некоторых положений настоящей Доктрины применительно к отдельным сферам деятельности общества и государства может быть осуществлена в соответствующих документах, утверждаемых Президентом Российской Федерации.

**Источник:** http://www.gtk.lissi.ru/doc.phtml?DocumentTypeID=6 (14.10.2011)

*М.С. ВЕРШИНИН*

# ПОЛИТИЧЕСКАЯ КОММУНИКАЦИЯ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ: ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ

В последние десятилетия мировое сообщество затронуто глобальным процессом перехода от индустриальной к информационной организации всей системы общественных отношений. Сложность и необычность новой эпохи требуют глубокого осмысления происходящих изменений.

Информационные технологии проникают во все сферы общественной жизни, но наиболее заметно их влияние в политике. В последние годы общественно-политический лексикон обогатился понятиями «электронное правительство», «киберполитика», «кибердемократия», «компьютеро-опосредованная политическая коммуникация», «цифровая (дигитальная) демократия», «коммуникационная демократия», «электронное гражданство» и др.

В России предметное поле исследований политической коммуникации в информационном обществе только складывается, и чрезвычайно важно выработать теоретико-методологические основания таких исследований с учетом российской специфики [1].

Активно внедряясь в сферу политики, новые информационно-коммуникационные технологии не только качественно видоизменили старые представления, установки, стереотипы, но и сломали многие формы поведения, модели взаимоотношений между политическими институтами и индивидами. По мнению А.А.Чеснакова, «начинается формирование нового обширного канала политической коммуникации, динамика развития которого может перевернуть представления как о системе обеспечения политической деятельности, такио традиционных инструментах политического участия» [2, с.65-66].

Среди перспективных направлений исследований политической коммуникации в информационном обществе выделим следующие:

### *1. Интернет и демократия*

Анализ роли Интернета в качестве гаранта демократии является одним из самых перспективных направлений в политической теории. Как утверждает Р.Даль, демократия уже прошла на практике через несколько революций, причем ее сторонники часто даже не вполне осознавали происходящее [3]. Л. Гроссман полагает, что с развитием новых коммуникативных технологий наступает новая, третья великая эпоха демократии [4, с. 527].

Информационные технологии изменяют не только форму осуществления демократических процедур, но с их внедрением меняется и сама суть развития социальных процессов.

В результате быстрого развертывания современных информационных технологий усилились дебаты относительно теории демократии. Острые дискуссии среди ученых и политиков вызывает вопрос о характере влияния Интернета на демократические институты и процессы (каково фактическое направление изменений, их сущность, интенсивность и глубина? Что происходит с прежними политическими институтами, когда и как рождаются новые институциональные структуры? Как изменить общественное устройство, чтобы максимально использовать преимущества новых возможностей в информационных взаимодействиях, но при этом сохранить устойчивость общественных институтов? Каковы механизмы трансформации взаимоотношений гражданского общества и государства, демократии и публичной сферы, прямой и представительной демократии в информационном обществе? В чем заключается влияние Интернета как средства массовой политической коммуникации на электоральное поведение граждан? Какой тип демократии формируется в информационном обществе? Какова природа электронной, компьютеро-опосредованной демократии (computer-mediated democracy) как новой формы политической коммуникации в информационном обществе? В чем состоит специфика «электронного правительства» как системы интерактивного взаимодействия государства и граждан при помощи Интернета,

новой модели государственного управления, преобразующей отношения граждан и властных структур?)

В исследовании темы «Интернет и демократия» можно выделить три основных подхода.

Один из них выражает так называемую "*популистскую точку зрения*"[5, 6], согласно которой Интернет восстанавливает возможность индивидуального воздействия на правительство и его политику. Э. Коррадо и Ч. Фейрстоун отмечают, что Интернет может обеспечить общение граждан с правительством "без посредников", а также уменьшить зависимость простых граждан от выборных должностных лиц, политических партий и группировок, отстаивающих свои экономические интересы"[7]. Интернет, посредством предоставления бóльших возможностей по обмену информацией, с одной стороны, усилит влияние простых граждан на политику, а с другой стороны, ослабит влияние тех, кому в настоящее время принадлежат средства массовой информации. То есть, чем больше возможности для граждан напрямую общаться с правительством, тем, вероятно, более вовлеченными в политику они будут, и чем больше их вовлеченность, тем сильнее будет их притягательность как личностей.

Суть популистской теории заключена в идее, согласно которой средства коммуникации являются фактором, отчасти определяющим степень политической активности избирателей. В настоящее время, сравнительно ограниченные для эффективного обмена политической информацией, средства массовой информации находятся в ведении политтехнологов, групп лиц, отстаивающих свои экономические интересы, а также прочих политических элит. Интернет, с популистской точки зрения, децентрализует доступ простых граждан к обмену информацией. Личное участие граждан в политике будет возрастать с ростом их влияния на общественную жизнь. Указанный процесс, получив достаточное развитие, приведет к трансформации общества.

Согласно так называемой *коммунитаристской точки зрения*, Интернет будет способствовать перестройке определяющих общественную жизнь связей между различными социальными слоями населения. Основная функция Интернета будет заключаться в формировании и развитии "сообщества". По мнению Х. Рейнгольда, "сообщество" создается тогда, когда люди взаимодействуют друг с другом в сети Интернет достаточно длительный период времени для того, чтобы развить прочные связи, а Интернет освобождает указанный процесс создания сообщества от ограничений, накладываемых физической удаленностью в пространстве"[8]. Подобное освобождение сообщества от ограничений, накладываемых географическим местонахождением, расширяет то, что в настоящее время называется локальным сообществом, до масштабов государства или всего мира в целом.

На этом ожидании строится более широкий спектр возможностей: увеличение взаимопонимания, большее уважение к точке зрения других людей, устранение дискриминации по расовому или половому признаку, создание общих ценностей. Если популистская теория касается изменений во взаимодействии граждан с правительством, то ожидания сторонников *коммунитаристской* теории основываются на усилении взаимодействия граждан между собой.

Концепция «*ускоренного развития плюрализма*» [9] строится на двух допущениях. Первое заключается в том, что увеличившиеся благодаря сети Интернет возможности получения и обмена информацией не изменят самой сущности плюрализма. На индивидуальном уровне Интернет никак не сможет изменить тот факт, что большинство людей чрезвычайно разборчивы в выборе политических проблем и средств получения информации. Они проявляют относительно сильный интерес лишь к небольшому числу политических проблем, оставаясь равнодушными ко всем остальным.

Второе допущение касается вопроса привлечения населения. Информационный поток и обмен информацией облегчают привлечение обывателей к участию в политическом процессе, а также организацию и осуществление политиками, активистами и другими заинтересованными лицами самого этого процесса. Кроме того, возможность широкого

доступа к информации ускорит развитие различных политических процессов. Более низкие издержки на организацию коллективных действий посредством Интернета будут наиболее выгодны для определенной группы населения, а именно той, которая либо находится вне рамок традиционных государственных и частных организаций, не вовлечена в бизнес, либо не входит в какие-либо профессиональные организации.

С точки зрения концепции "*ускоренного развития плюрализма*", Интернет способствует существующему дроблению современной политической системы в соответствии с экономическими интересами политических групп и переходу к гибкой системе, основанной на различных стратегиях влияния политических групп, менее зависимых от общественных институтов и организаций.

Интернет будет оказывать серьезное влияние на политическую жизнь общества, несмотря на то, что имеется множество причин теоретического и практического свойства, которые заставляют усомниться в существовании непосредственной связи между изменениями в сфере коммуникационных технологий и политической активностью населения. Есть серьезные основания полагать, что Интернет будет содействовать децентрализации контроля над частными средствами массовой информации, препятствуя тенденции укрупнения средств массовой информации.

Исследователи видят перспективы в потенциале Интернета, и не только в том, чтобы сделать политическую связь и поток информации более эффективными и прозрачными, но также, чтобы использовать любой удобный случай для участия граждан в политических процессах. Наиболее значительными являются:

- Более эффективное управление посредством эффективных организационных действий
- Более эффективная связь между политикой и гражданами
- Активация и мотивация, направленные на вовлечение граждан в политику за пределами Интернета посредством самого Интернета
- Более практичные политические решения вследствие объединения знаний граждан, основанных на опыте.

Указанные примеры описывают, однако едва ли исчерпывают, предлагаемые со стороны Интернета реальные возможности для политических изменений. Одни из этих изменений явятся прямым следствием появления новых технологий, другие проявят себя в качестве создания новых политических институтов, которые под влиянием использующих Интернет граждан, групп, а также самих чиновников произведут, в свою очередь, изменения в политической жизни общества.

### *2. Электронная демократия как компьютеро-опосредованная форма политической коммуникации*

Что подразумевается под термином «электронная демократия»? Термин стал часто употребляться теми, кто использует компьютерные технологии в политическом процессе. Однако прилагательное «электронный» является не совсем точным. Оно может также относиться к использованию электронного микрофона или телевидения. В некоторых случаях более точным был бы термин «цифровая демократия»(«digital democracy»). Возможны, также, другие термины: «кибердемократия», «виртуальная демократия», или «демократия века информационных технологий». Однако в настоящее время чаще применяется термин «электронный», который подразумевает «применение интерактивных технологий». Поэтому в статье я тоже буду использовать термин «электронная демократия» как основной.

Концепции электронной демократии относятся к теориям, которые рассматривают компьютеры и/или компьютерные сети в качестве важнейшего инструмента в работе демократической политической системы. «Электронная демократия» - это любая демократическая политическая система, в которой компьютеры и компьютерные сети используются для выполнения важнейших функций демократического процесса, таких как распространение информации и коммуникация, объединение интересов граждан и принятие

решений (путем совещания и голосования). Эти концепции отличаются по возможности использования прямой или репрезентативной формы демократического правления и по степени активности граждан в государстве. Общим у этих концепций является уверенность в том, что различные свойства новых средств информации, такие как интерактивность, более быстрые способы передачи информации, возможности связи большого количества пользователей друг с другом, изобилие информации и новые пользовательские возможности по управлению процессами могут положительно влиять на демократическую политическую систему.

Во многих западных исследованиях основной целью электронной демократии декларируется повышение уровня политического участия [10].

Следует заметить, что массовое политическое участие - лишь одна из множества ключевых функций политики средствами Интернета. Равными по значимости функциями Интернета, способными усилить институты представительной демократии, являются: обеспечение условий для конкуренции партий и соревнования кандидатов, активизация и привлечение гражданского общества, обеспечение прозрачности и повышение ответственности в процессе принятия решений, а также их эффективное доведение от властных структур до граждан. Для переходных (транзитных) обществ (Россия в их числе) эти функции даже более важны, чем уровень массового участия.

Выборные демократии могут способствовать высоким уровням явки избирателей, но другие политические права и гражданские свободы сведутся к показухе, если:

- гражданское общество останется слабым и разрозненным,
- представительные институты будут недостаточно объединены и согласованы,
- соревнование между партиями, осуществляемое избирателями посредством реального выбора кандидатов сведено к минимуму, власть поражена коррупцией,
- попирается закон,
- подавляются оппозиционные движения.

На наш взгляд, предмет изучения (а именно: характер влияния Интернета на демократические институты и процессы) в переходных обществах отличается от общепринятого в предшествующей литературе в США и Западной Европе, где часто полагают, что Интернет только усилит демократию, если увеличатся возможности политического участия, такие, как: влияние граждан на принятие решений, участие в процессе обсуждения политического курса или электронное голосование (многие теоретики электронной демократии приходят к заключению, что если Интернет слабо способствует выполнению этих функций, то цифровые технологии будут иметь минимальное влияние на демократию или демократизацию). По нашему мнению, это слишком ограниченный взгляд. Более приемлем подход (особенно если речь идет о переходных обществах), согласно которому информационные технологии могут усилить институты представительной власти и гражданского общества.

Идеи формирования эффективного гражданского общества с опережающим развитием горизонтальных связей между избирателями приобретают необходимую материальную базу с развитием электронных, компьютеро-опосредованных коммуникаций.

Ключевой вопрос при оценке роли информационных технологий для демократии состоит в том, насколько правительства и гражданское общество научатся использовать возможности, предоставляемые новыми каналами информации и коммуникации, чтобы продвигать и усиливать базовые представительные институты, объединяющие граждан и государство. При таком рассмотрении возможности для общественного участия, создаваемые посредством новой технологии, безусловно важны, но Интернет способен и генерировать информацию, усиливая прозрачность, открытость деятельности и ответственность властных органов национального и межнационального уровней, а также укреплять каналы интерактивного общения между гражданами и посредническими институтами. Это особые функции, Интернет реализует некоторые из них лучше, чем любые другие средства. В частности, Интернет мог бы:

- предоставить более подходящие средства для взаимодействия в политических кампаниях партиям меньшинства, чем традиционные массовые средства информации (газеты, радио, телевидение);
- обеспечивать более широкий единовременный доступ к информации для журналистов к официальным документам и текущим законодательным инициативам и предложениям;
- способствовать усилению внутренней организации партий и взаимодействия членов партий и др.

Нельзя оставлять без научного анализа проблемы, связанные с опасностями и рисками электронной демократии, в частности:

- опасность манипулирования данными голосований и выборов из-за отсутствия достаточной защиты данных,
- опасность разделения общества на тех, кто владеет информацией, и тех, кто не владеет (цифровое разделение), и, как следствие, ущемление принципа демократии выбора,
- опасность пропаганды преступных и экстремистских группировок и их влияние, особенно на молодое поколение.

Наибольшие перспективы в России имеет процесс использования Интернет-технологий для дальнейшего расширения возможностей существующий системы представительной демократии и развития процессов «электронной демократизации». Ее основной смысл заключается в использовании Интернета для следующих целей: 1) расширения доступа избирателей и СМИ к законотворческой деятельности; 2) снижения издержек по формированию ассоциаций и объединений избирателей; 3) повышения эффективности обратных связей между избирателями и их представителями в законодательных органах власти.

### *3. Электронное правительство*

Дискуссия об электронной демократии в последние годы смещается в сторону обсуждения проектов электронного правительства.

В российском случае электронное правительство означает в первую очередь повышение эффективности механизмов контроля государства над гражданами в сферах сбора налогов, борьбы с преступностью и т.д. [11, с.37]. В федеральной целевой программе «Электронная Россия на 2002-2010 гг.» под электронной Россией понимаются федеральные и региональные органы власти, министерства и ведомства, комиссии и комитеты. Западный подход подразумевает, помимо облегчения коммуникации, усиление контроля граждан над правительством, что связано, в первую очередь, с введением публичных оценочных показателей деятельности последнего. Ни одной подобной программы в России нет и не разрабатывается. Даже в проекте «Глобальный портал развития», являющийся частью проекта Всемирного банка, реализация электронного правительства проходит через последовательные этапы одностороннего информирования граждан, предоставления сервисов, и лишь затем создание систем взаимодействия граждан и власти.

Нам представляется, что реальной проблемой российского государства на ближайшие годы становится не создание электронной власти, но формирование информационного дизайна, который бы позволил в будущем успешно бороться с разделением общества и информационными разрывами между центром и регионами. Можно сказать, что институциональный дизайн включает в себя формирование единого информационного поля государства.

Проекты создания «электронного правительства» породили дискуссию: обязательно ли информационное общество является в то же время открытым и гражданским? По-видимому, это необязательно. Вполне возможно, что такое информационное общество, насыщенное информатизацией, не будет открытым и даже гражданским.

Обязательно ли информатизация спасает нас от авторитаризма?

Безусловно, государство заинтересовано насытить информационными технологиями свои службы, чтобы те могли более оперативно и качественно принимать решения. В первую

очередь службы с повышенной долей ответственности, а также связанные с осуществлением учета различного вида: материальных ресурсов, физических и юридических лиц, их доходов. Так автоматизация делает общество прозрачнее для государства. А встречного движения пока не видно. И этот процесс таит в себе немалую опасность, особенно в нашей стране, где уровень доступа населения к современным технологиям крайне низок.

Представляется, что для России крайне актуальна проблема “нового деспотизма”, т.е. изощренно-рафинированных форм манипулирования обществом с помощью современных технологий коммуникаций, массовой культуры, политического процесса. “Новый деспотизм” не прибегает к открытому насилию, подавлению прав личности, упразднению демократических институтов. Конструкция либеральной демократии сохраняется, но ее содержание (функции гражданского волеизъявления) выхолащивается. “Новая технология, - пишет Б.Барбер, - может стать опасным проводником тирании... Более опасной тирании, чем невидимая и мягкая, не существует. Такая тирания, в которой подданные становятся соучастниками своего собственного жертвоприношения и в которой порабощение является результатом не намерений, а обстоятельств. Технология не должна неизбежно разрушить демократию, но ее потенциал для “милостивого” господства не может игнорироваться” [12, p. 581-582].

Как удачно выразился исследовавший это явление Б. Капустин, “новый деспотизм” “выводит жизнь людей за рамки политического бытия”[13, с.229].

Если информатизация бурно развивается "наверху", не проникая в общество, она лишает граждан возможности следить за деятельностью госструктур, проверять их, а значит, не только не делает государство прозрачнее, но и может усилить монополию государства на информацию. Электронизация "сверху" даст в руки правящей элиты дополнительные возможности манипуляции обществом и отдельным человеком.

Технология может изменить методы регулирования, но не меняет их сути. Информационная открытость не станет прямым следствием оцифровки отношений граждан и государственных институтов и вряд ли приведет к либерализации общественных отношений. Кстати, это показывает и опыт Сингапура - страны отнюдь не демократической, однако лидирующей по эффективности использования систем e-government. Примеров разительного контраста между уровнями социального и технологического развития государств во всём мире – сколько угодно. Даже рядом не стоявшие с демократией султанат Бруней, Сингапур, Малайзия, королевство Саудовская Аравия, княжество Дубай и Объединённые Арабские Эмираты уже сегодня располагают таким уровнем развития IT, которого по планам проекта «Электронная Россия» у нас не будет даже в 2010-м году. Гражданское же общество в большинстве этих стран находится где-то на стадии раннего феодализма.

Электронная революция не способна сделать полицейское государство более открытым. Никакой – самый замечательный IT-проект – не сможет стать протезом демократии. Напротив, благодаря технологии общество становится все более прозрачным для власти, а значит, более контролируемым. Плохо функционирующее государство отнюдь не станет лучше благодаря электронному правительству. Отсталое общество не перескочит из посттоталитарного в демократическое из-за того, что население получит доступ к тем или иным информационным ресурсам. Это опасные иллюзии, но они, к сожалению, достаточно широко распространены в России.

**Литература:**

1. См.: Вершинин М.С. Политическая коммуникация в информационном обществе. СПб., 2001

2. Чеснаков А.А. Ресурсы INTERNET и российские политические технологии: состояние и перспективы развития // Вестник МГУ. Сер.18. Социология и политология. 1999. №4

3. См.: Dahl R. A. Democracy and Its Critics. New Haven: Yale University Press, 1989

4. См.: Соловьев А.И. Политология: Политическая теория, политические технологии. М., 2000

5. Grossman L.K. The Electronic Republic: Reshaping Democracy in the Information Age. New York: Viking, 1995

6. Browning G. Electronic Democracy: Using the Internet to Influence Politics. Wilton, CT: Online Inc., 1996

7. Corrado A., Firestone Ch., eds. Elections in Cyberspace: Toward a New Era in American Politics. Washington, DC: Aspen Institute, 1996

8. Rheingold H. "A Slice of Life in my Virtual Community," in *Global Networks*, ed. L. M. Harasim. Cambridge, MA: MIT Press, 1993

9. Bimber B. The Internet and Political Transformation: Populism, Community, and Accelerated Pluralism // Polity. Vol. XXXI. № 1

10. Подробнее см.: Вершинин М.С. Электронная демократия как компьютеро-опосредованная форма политической коммуникации // Материалы международной научно-практической конференции "Коммуникация: теория и практика в различных социальных контекстах" - "Коммуникация-2002" ("Communication Across Differences"). Ч.1. Пятигорск, 2002

11. См.: Песков Д.Н. Интернет в российской политике: утопия и реальность // Полис. 2002. № 1

12. Barber B. Three Scenarios for the Future of Technology and Strong Democracy // Political Science Quarterly, Winter 1998-1999. Vol. 113. № 4

13. Капустин Б.Г. Современность как предмет политической теории. М., 1998

**Источник:** "Актуальные проблемы теории коммуникации". Сборник научных трудов. - СПб. - Изд-во СПбГПУ, 2004. - С. 253-270.

*МИХЕЕВ А.Н.*

# НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ДИПЛОМАТИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ: НЕКОТОРЫЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Новые информационные технологии (ИТ), изменившие практически все сферы человеческой жизни, не могли не затронуть и область внешней политики, дипломатии. Как за рубежом, так и в России все чаще в документах и выступлениях официальных лиц звучит мысль о том, что "осуществление внешней политики как никогда зависит от управления информацией и информационных технологий"[76], а "владение новейшими информационными технологиями" становится необходимым условием эффективной работы дипломатов[77]. Внешнеполитические ведомства разных стран (Великобритании, США, Канады и др.) активно внедряют в свою деятельность разнообразные ИТ, перестраивают свою работу таким образом, чтобы максимально повысить ее эффективность за счет использования новых технологий. Спектр мнений о возможной роли ИТ в труде дипломата весьма широк: от радикальных, утверждающих, что с развитием технологий фигура дипломата вообще отойдет на второй план, станет ненужной, до консервативных, видящих в новых технологиях лишь усовершенствованный аналог бумажных архивов и печатных машинок. Вероятно, истина, как это часто бывает, лежит посередине: дипломатия не может обойтись без человека, она основывается во многом на личных контактах, но новые технологии могут и должны помочь дипломатам более эффективно выполнять свои функции.

По словам бывшего ректора Дипломатической академии МИД РФ Ю.Б. Кашлева, "нет нужды доказывать те преимущества, которые могут дать дипломату в его практической работе за рубежом или в центральном аппарате новейшие информационные технологии. Это и оптимизация поиска необходимой информации через компьютерные сети, и моментальные ее получение и обработка. Столь же молниеносно информация может передаваться между Центром и загранучреждениями и использоваться по назначению. Для дипломатической работы большое значение имеет то, что с Интернетом отпадает необходимость траты времени на написания многостраничных справок по тем или иным проблемам — ты можешь получить все нужное через свой компьютер в любой момент. Человек не может одинаково хорошо знать все — и искусство дипломатии, и иностранные языки, и военные вопросы, и экономику, а компьютер помогает восполнить пробелы в знаниях… Возможности использования новой информационной технологии на направлении международных отношений поистине безграничны — информационная поддержка подготовки и принятия решений, внешнеполитическое прогнозирование, просчет многовариантного развития обстановки, оптимизация системы управления"[78].

Очевидно, что это описание ставит своей целью скорее краткий общий обзор рассматриваемой проблемы, а потому объединяет вместе самые различные сферы применения ИТ и известным образом упрощает ситуацию. К примеру, с утверждением автора, что с помощью Интернета "ты можешь получить все нужное через свой компьютер в любой момент", можно поспорить. Тем не менее, в приведенной цитате упоминаются многие важные направления использования новых технологий в дипломатической работе. Настоящая статья представляет собой попытку определенным образом их систематизировать.

Вероятно, не стоит посвящать много внимания рассказу о возможностях поиска и передачи информации, которые предоставляют новые технологии. Интернет, поисковые системы, электронная почта, мобильные телефоны, возможность дистанционной работы и даже автоматизированный перевод, который хотя и далек от совершенства, но позволяет

[76] U.S. Department of State Strategic Plan. September 2000. (http://www.state.gov/www/global/general_foreign_policy/2000_dos_stratplan_body.pdf). P. 89.

[77] См. Выступление Министра иностранных дел Российской Федерации И.С.Иванова в МГИМО (У) по случаю начала нового учебного года (1 сентября 2000 года) (http://www.rg.ru/oficial/from_min/mid/1132.htm).

[78] ***Кашлев Ю.Б.*** На передовом рубеже глобализации. Международное информационное общество и вызовы дипломату XXI века//"Независимая газета", 28 декабря 2000 г.

дешево и быстро просматривать большие объемы информации[79], давно уже стали частью повседневной жизни и были приняты на вооружение бизнесом. По поводу внедрения этих технологий не возникает вопросов даже у самых больших консерваторов — с их точки зрения, это всего лишь усовершенствованный вариант печатных машинок, бумажных архивов и телеграфа, к тому же, не связанный со спецификой дипломатической деятельности.

Стоит отметить, впрочем, что, по закону перехода количественных изменений в качественные, внедрение новых технологий изменяет не только скорость выполнения отдельных операций, но и сам характер деятельности. Известно, что скорость нахождения нужной информации или передачи большого количества ее иногда имеет принципиальное значение (в особенности в дипломатической деятельности, например, в условиях международного кризиса). Во-вторых, важно отметить, что новые ИТ отнюдь не просто копируют существовавшие до того технологии. Даже электронная почта (не говоря уже о возможности передавать информацию в иных, чем текст, форматах, групповом программном обеспечении, видеоконференциях), как свидетельствуют исследователи, существенно отличается от телеграфа по свойствам и влиянию на характер дипломатической деятельности. А современный "интеллектуальный" поиск с помощью специальных программ (knowbots) столь же отличен от всевозможных систем индексов, применяемых в бумажных архивах.

Итак, некоторые технологии, уже ставшие неотъемлемой частью повседневной жизни, постепенно меняют и повседневных труд сотрудников дипломатических ведомств. С другой стороны, в определенных областях внешнеполитической деятельности применение новых технологий пока еще находится на стадии экспериментов, однократного применения, как, например, при ведении переговоров. Этот вид деятельности традиционно считается основанным исключительно на личном контакте и с древнейших времен претерпел мало изменений, несмотря на развитие технологий. Однако, как указывает директор "Диплопроекта" Средиземноморской академии дипломатических наук Джован Курбалийя, в некоторых ситуациях Интернет может стать более предпочтительным средством ведения переговоров, чем личный контакт. Во-первых, когда личная встреча требует поездки, нежелательной по каким-либо соображениям (времени, безопасности, и т.д.). Например, встреча Всемирного банка в Барселоне не состоялась из-за возможных протестов антиглобалистов, а была проведена по Интернету. Во-вторых, при необходимости уменьшить "эмоциональный шум", появляющийся при личном контакте. Обычно недостаток эмоциональности считается негативным аспектом, однако иногда переговоры бывают излишне "эмоционально нагружены", и тогда приходится вести их через посредников, как на переговорах по бывшей Югославии в Дейтоне и Рамбуйе. В таких случаях отсутствие личного контакта может сыграть положительную роль — переговоры через Интернет. В-третьих, общение через Интернет, с помощью технологий "groupware" и гипертекста помогает более детально сосредоточиться на тексте соглашения, проработать больше нюансов[80]. Наконец, весьма показателен пример с переговорами в Дейтоне, когда представителям сербов был предложен "виртуальный полет" над спорной территорией между Горажде и Сараево. После этого споры были решены в течение нескольких минут. Как пишут стратегические аналитики Д. Кюл и М. Либики, "наиболее значительным результатом, вероятно, было установление "информационного преобладания" над сербскими переговорщиками… Американские участники переговоров, по сути сказали: "мы знаем, где вы живете, и, как видите, можем сделать это своей целью"[81].

Одним из перспективных направлений использования ИТ, по мнению некоторых авторов, является их роль в организации дипломатической деятельности в русле весьма

[79] Reinventing Diplomacy in the Information Age. A Report of the CSIS Advisory Panel on Diplomacy in the Information Age. (http://www.csis.org/ics/dia/). P. 15.
[80] ***Kurbalija, Jovan.*** Internet and Negotiations// Second International Conference on Web-Management in Diplomacy. Malta, 1-3 February 2002.
[81] Reinventing Diplomacy in the Information Age. P. 44.

популярной в мире бизнеса (и привлекающей все большее внимание в других сферах, в том числе в дипломатии) концепции “управления знаниями”. Чтобы лучше понять, как можно применить эту концепцию к сфере дипломатии, исследователи предлагают разделить все “дипломатические процессы” на три группы. Первая — это в большой степени, повторяющиеся и стандартные процессы — те, которые следуют определенной четкой последовательности действий; каждый шаг предсказуем. Большинство этих процессов связано с консульской деятельностью типа выдачи виз или паспортов. Этапы их выполнению включают заполнение форм, запрос рекомендаций у других департаментов, проверку досье, выдачу визы или паспорта, и т.д. Эти процедуры легко могут быть переведены в компьютерные алгоритмы и упрощены с помощью специально разработанных компьютерных приложений, так что вмешательство сотрудников будет минимальным. То же можно сказать и о решении различных административных вопросов.

Бóльшая часть дипломатических действий относится к категории частично повторяющихся задач. В первую очередь такие задачи связаны с многочисленными международными режимами, существующими в области окружающей среды, торговли, прав человека и т.д. Каждый из них обладает определенным механизмом, основанным на международных соглашениях, через который организуются регулярные встречи, обрабатываются документы, контролируется выполнение соглашений и т.д. Эти действия осуществляются на более или менее регулярной основе. Отчетная документация подготавливается к определенным срокам; встречи различных комитетов организуются неоднократно более или менее стандартным способом. Таким образом, форма периодически повторяется, в то время как содержание изменяется в зависимости от ситуации. Периодически повторяющиеся аспекты такой деятельности идеальны для автоматизации. Кроме того, продвинутые методы “управления знаниями” могут быть использованы для сохранения и использования опыта, накопленного в той или иной сфере.

Последняя группа действий, связанных с дипломатией - неповторяющиеся действия. Это — “сливки” дипломатической деятельности, состоящие главным образом из переговоров по многосторонним и двусторонним вопросам, нацеленных на разрешение международных кризисов или двусторонних проблем, установление новые двусторонних и многосторонних режимов и т.д. Эти процессы требуют много информации и знаний, которые не могут быть сведены к определенным логическим структурам. Однако программы “управления знаниями” высокого уровня могут играть важную роль и в этом случае, помогая в принятии решений и, особенно, в “улавливании” и использовании опыта, вырабатываемого в этих видах деятельности. Как известно, специалисты-практики на основе своего практического опыта вырабатывают собственные правила внешнеполитического анализа, принятия решений и пр., позволяющие им добиваться успеха[82]. Современные “обучающиеся” программы, нацеленные на “вытягивание” из экспертов их знаний, могут сделать по крайней мере часть этого опыта доступной широкому кругу дипломатов.

Отдельного внимания заслуживает роль новых информационных технологий непосредственно в процессе принятия решений по различным вопросам внешней политики. Как указывает американский политолог А. Джордж, качество принимаемых решений напрямую зависит от следующих факторов: доступа к необходимой информации и возможностей ее адекватного анализа; четкого определения целей того или иного внешнеполитического шага; обеспечения относительно широкого спектра различных вариантов действия; анализа возможных последствий воплощения каждого из альтернативных вариантов; способности извлекать уроки из опыта прошлого[83]. Весьма распространена точка зрения, что компьютеры нужны только для сбора и предварительной

---

[82] ***Севостьян И.П.*** Планирование внешней политики в США. Некоторые вопросы теории, практики и организации. М.: Международные отношения, 1974. С. 157.

[83] ***Колобов О.А., Корнилов А.А., Макарычев А.С., Сергунин А.А.*** Процесс принятия внешнеполитических решений: исторический опыт США, государства Израиль и стран Западной Европы. Нижний Новгород, изд-во Нижегородского университета, 1992. С. 137.

обработки информации, однако они не могут помочь руководителю при принятии решений[84]. Более детальное изучение вопроса показывает, однако, что современные информационные технологии могут оказать помощь практически на всех стадиях принятия решения (имеется в виду решение вообще, а не конкретно в области внешней политики), в том числе с точки зрения пяти критериев, выделяемых А. Джорджем. Рассмотрим этот вопрос более детально.

Средства интеллектуальной поддержки деятельности специалисты подразделяют на три группы: интеллектуальные информационно-поисковые системы (ИПС), обеспечивающие диалоговое взаимодействие непрограммирующих пользователей с базой данных и знаний на профессиональных языках пользователей (близких к естественному); расчетно-логические системы, позволяющие непрограммирующим пользователям решать в диалогическом режиме свои задачи с использованием сложных математических методов и моделей; экспертные системы, позволяющие осуществлять эффективную компьютеризацию областей, в которых знания могут быть представлены в экспертной описательной форме, но использование точных математических моделей затруднительно[85].

**К первой группе** относятся разнообразные ИПС с более или менее "интеллектуальными" возможностями поиска: разнообразные автоматизированные архивы, банки данных и пр. К этой же категории можно отнести и всю сеть Интернет в целом, в особенности с учетом возможностей поиска (в том числе "интеллектуального") — хотя в данном случае речь не идет о "базе данных и знаний на профессиональных языках пользователей". Стоит отметить, однако, что в современных условиях избытка информации этап поиска и сбора информации приобретает новое измерение. Более правильно было бы рассматривать этот этап как управление информацией: процесс, который начинается со сбора данных и заканчивается предоставлением ЛПР необходимой для принятия решения информации (необходимо помнить о том, что понятия "данные" и "информация" отнюдь не тождественны). Обычно в этом процессе в той или иной форме используются следующие основные приемы: *контекстуализация*, т.е. помещение того или иного факта в определенный контекст; *"добыча данных"* (data-mining), т.е. получение необходимой информации с помощью обработки большого массива данных на компьютере (например, получение информации о том, склонна ли определенная страна поддерживать США при голосовании в Генеральной Ассамблее ООН, из огромного объема результатов голосований); и наконец, *конденсация*, т.е. представление информации насколько возможно кратко, не теряя при этом содержащегося в ней смысла. Хотя все эти приемы не новы (например, "добычу данных" теоретически возможно было осуществлять и без использования вычислительных машин, хотя это требовало чрезвычайно длительных вычислений; а конденсация традиционно проводилась в виде составления рефератов), использование НИТ позволило существенно повысить их эффективность[86]. Например, контекстуализация приобретает иной характер вид с использованием "группового программного обеспечения", возможностей передачи мультимедийной информации. Теперь она уже не ограничивается только рамками одного подразделения, но даже одного ведомства. Например, одно из главных направлений информатизации внешнеполитического сообщества США — объединение всех агентств, работающих за рубежом, всего персонала посольств в единую команду. Стоит отметить также, что нововведения касаются не только применения ЭВМ, но и новых технологий организации информации, таких, как гипертекст. К тому же в определенной степени контекстуализация, "добыча данных" и консолидация все в большей степени могут осуществляться полностью автоматизированно, по мере того, как эволюционируют компьютерные программы. Как отмечал в своей статье "Дипломатия в эпоху информационных технологий" секретарь Совета по информационной работе МИД РФ О.Б. Озеров, будущее — "за программами, которые способны, подключаясь к международным

[84] ***Ларичев О.И., Мошкович Е.М.*** Качественные методы принятия решений. Вербальный анализ решений. М., Наука, 1996. С. 201.
[85] ***Поспелов Г.С.*** Искусственный интеллект — основа новой информационной технологии. М., Наука. 1988.
[86] ***Jovan Kurbalija***. Knowledge Management and Diplomacy
**(**http://diplo.diplomacy.edu/Knowledge/Management/management.htm).

сетям, например к Интернет, “вытягивать” из них наиболее ценную и значимую информацию, препарировать ее, проводить контент-анализ не только первого, но и второго уровня и подавать на стол уже почти готовое “информационное блюдо”. Наиболее передовой “софтвер” способен самостоятельно подготовить справку по документу, небольшой автореферат по заданным параметрам”[87].

**Ко второй группе** следует отнести различные программы для моделирования международных процессов, а точнее те из них, которые позволяют пользователю, не знакомому со структурой программы, общаться с ней на естественном или профессиональном языке и получать результаты моделирования в диалоговом режиме. В 60-е—70-е годы, период “компьютерного бума”, с возможностями подобных программ связывались порой ожидания кардинальных перемен в мировой политике. Так, известный специалист по математическому моделированию кризисных ситуаций и гонки вооружений, американский математик Т. Саати писал в середине 70-х гг. в книге “Математические модели конфликтных ситуаций”: “При условии, что в будущем войны еще будут иметь место, вероятно, противники будут анализировать их на вычислительных машинах с большой точностью, а не сражаться на поле боя… На вычислительных машинах будет разобрано множество вариантов, возможно тысячи, для анализа всевозможных изменений и нюансов, какие только смогут предвидеть политические и военные лидеры стран-участниц”[88]. Эйфория довольно быстро сменилась разочарованием, и под вопрос была поставлена не только перспектива замены реальных войн компьютерными, описанная Т. Саати, но и сама возможность использования компьютеров для моделирования и прогнозирования международных процессов. Связано это было, во-первых, с проблемой применимости понятий “законы” и даже “закономерности” к международным отношениям, а во-вторых, даже при признании наличия закономерностей, “с трудностями математической формализации социально-политического и международно-политического материала”[89] и выражения найденных закономерностей в виде компьютерных программ, с “невозможность квантифицировать волевые, моральные и иные компоненты”[90]. Тот же Саати отмечал, что “международная политика настолько сложна, что никакой математический подход не в состоянии должным образом учесть все существенные элементы, обуславливающие принятие политических решений”[91].

С другой стороны, как указывали сторонники применения ЭВМ для анализа международных процессов, хотя “далеко не все явления общественной жизни можно выразить языком математики,… этого, собственно говоря, и не нужно. Самое главное — выразить те параметры общественных систем, которые необходимы для эффективного управления, т.е. массовые, устойчивые, повторяющиеся отношения и функции”[92]. “Как известно, применение количественных методов в социальных науках базируется на создании таких моделей, которые по своей сути зависят не столько от абсолютных значений цифр, сколько от их порядка… Такие модели предназначены не для получения численных результатов, а для ответов на вопросы, имеет место или нет некоторое свойство, например, устойчивость[93].

Как бы то ни было, многочисленные попытки моделирования международных и внутриполитических процессов продолжают делаться как в рамках самих внешнеполитических ведомств, так и (особенно активно) в связанных с последними исследовательских центрах; а подобные программы играют все более важную роль среди интеллектуальных средств поддержки принятия решений.

---

[87] ***Озеров О.Б.*** Дипломатия в эпоху информационных технологий// Международная жизнь, №4, 1997. С. 56-57.
[88] ***Саати Т.*** Математические модели конфликтных ситуаций. М., Советское радио, 1977. С. 285-286.
[89] ***Гришин А. В., Никольский Н. М.*** Системный анализ и диалог с ЭВМ в исследовании международных отношений. Некоторые вопросы теории и опыта. М.: Международные отношения, 1982. С. 114-115.
[90] ***Воронцов Г.А.*** Буржуазная наука на службе политики. М.: Международные отношения, 1975. С. 145.
[91] ***Саати Т.*** Ук. соч. С. 112.
[92] ***Афанасьев В.Г.*** Научное управление обществом (опыт системного исследования). М., Политиздат, 1973. С. 341-342.
[93] ***Саати Т.*** Ук. соч. С. 20.

Наконец, **к третьей группе** относятся так называемые экспертные системы. В целом они классифицируются на диагностирующие, системы мониторинга, прогнозирующие, планирующие, проектирования, управления, обучения, интерпретирующие. Можно сказать, что такие системы — это программа для ЭВМ, которая: строит рассуждения с помощью как символических, так и математических знаний о предметной области; использует присущие данной предметной области эвристические и точные методы; работает на уровне специалистов в данной предметной области; объясняет свои знания и рассуждения и обладает необходимой гибкостью, т.е. возможностью настройки и пополнения знаний о предметной области. Основной подсистемой, отличающей экспертные системы от других систем искусственного интеллекта, является система объяснения, которая делает экспертную систему "прозрачной" для пользователя, а значит понятной и принимаемой в качестве средства подготовки решений[94].

Характеризуя отечественную разработку в области экспертных систем для внешнеполитической деятельности — систему "Ариадна+", созданную в Научно–исследовательском центре информатики (НИЦИ) при МИД РФ,— ее авторы пишут: "Ее назначение — обеспечение и поддержка функционирования информационно–аналитической службы, эффективная работа с противоречивой информацией, формирование формализованных моделей, характеризующих исследуемую предметную область (политическая, экономическая и социальная системы, корпоративная безопасность и др.), качественная и количественная оценка исследуемых процессов и проблем". По их словам, система может выступать в качестве "усилителя естественного интеллекта". "На практике система выступает как опосредующее звено процесса взаимодействия с реальностью, и ее основная функция сводится в конечном счете к способствованию порождения пользователем некоторых гипотез о структуре исследуемой системы, принципах ее функционирования и аргументации данных гипотез"[95].

Особая функция экспертных систем (или особого вида экспертных систем) состоит в том, что они не просто предоставляют лицу, принимающему решения, необходимую информацию (в том числе результаты расчетов и моделирования), но и направляют его по определенным этапам процесса принятия решения, а порой и сами проходят их вместо ЛПР. С точки зрения психологии, "процессы принятия собственно интеллектуальных решений не являются однородными, они могут быть жестко алгоритмического, эвристического или продуктивного (творческого) типа"[96]. Очевидно, что в принятии решений, относящихся к первому из названных классов, роль компьютера может быть весьма велика, а в последнем случае — напротив, очень ограничена. Особый интерес представляет принятие решений эвристического типа, когда компьютер, направляя человека по установленным этапам, помогая ему ставить правильные вопросы, предлагая варианты решения отдельных ситуаций, может ускорить и сделать более успешным нахождение самим человеком (NB!) оптимального решения. Как отмечают отечественные исследователи вопросов принятия решений О.И. Ларичев и Е.М. Мошкович, "современные средства анализа вариантов и подготовки решений нацелены на то, чтобы "заострить" интуицию руководителя. Естественно, компьютер не может вывести правильное решение, как он выводит теоремы, но он может подсказать, при каких условиях решение приведет к нежелательным последствиям"[97]. Как следует из результатов проведенных в этой области исследований,

---

[94] ***Беляев И.П., Трофимов Е.А.*** Системы поддержки принятия решений. Часть 2. Интеллектуальные системы поддержки принятия решений: Обзоры по электронной технике. Сер. 9. Экономика и системы управления. — М., ЦНИИ "Электроника", 1990. С. 12.

[95] ***Кретов В.С, Фролов И.В.*** Компьютерный анализ политических ситуаций и конфликтов// Тезисы международной конференции "Информационные технологии, безопасность и разрешение конфликтов". 28-30 апреля 1998 г., Центр Политических и Международных Исследований (ЦПМИ) (http://isn.rsuh.ru/cpis/win/konfer/98_04/kretov.htm).

[96] ***Корнилова Т.В., Тихомиров О.К.*** Принятие интеллектуальных решений в диалоге с компьютером. М., Изд-во МГУ, 1990. С. 18. Аналогичным образом американский исследователь Г. Саймон делит все решения на "программируемые" и "непрограммируемые" — см. ***Бурлацкий Ф.М.: Галкин А.А.*** Политика, социология, международные отношения. М.: "Международные отношения", 1974. С. 232-233.

[97] ***Ларичев О.И., Мошкович Е.М.*** Качественные методы принятия решений. С. 201.

“выбор готового решения при наличии подсказок доминируется наличием собственного решения и его близостью к одной из подсказок (выделение мое — А.М.). В сложных же ситуациях (при неоднозначности собственного решения) наличие процедуры перебора вариантов решения позволяет за счет предъявления ЛПР ограниченного множества альтернатив решения увеличить успешность его принятия практически в 1,5 раза. В связи с этим данная процедура может быть рекомендована в некоторых случаях в качестве метода повышения эффективности принятия решений в условиях автоматизации деятельности”[98].

Таким образом, современные системы поддержки принятия решений на различных этапах процесса принятия решений могут выполнять разнообразные функции. Однако важно еще раз отметить, что любые системы, даже самые сложные, лишь помогают принимать решение — основная роль по-прежнему остается за человеком. “Следует подчеркнуть,— отмечает в предисловии к упоминавшейся выше книге Т. Саати И.А. Ушаков,— что сложные и ответственные решения определяются огромным числом самых различных факторов, не все из которых могут быть учтены при построении соответствующих математических моделей. Кроме того, многие решения, оптимальные в смысле тех или иных количественных критериев, не могут быть приняты в силу существующих политических, моральных или этических установок стороны, принимающей решения… информация должна лишь помочь специалисту в той или иной области, а не заменять решение: принятие решений в конечном счете остается прерогативой человека”[99].

Как отмечают авторы многих исследований, по мере того как рутинные задачи все более берет на себя новая технология, в дипломатической деятельности возрастает роль человека, его творческого начала, реализации которого также может помочь правильное, системное использование ИТ[100]. Изменяется роль дипломата — он становится не просто поставщиком оперативной информации для своего правительства (с этой функцией порой гораздо лучше справляется телевидение), а “посредником и аналитиком, способствующим обмену информацией и быстрому принятию решений”[101]. “От посольства требуется не столько сообщение о том или ином факте, сколько анализ происшедшего и прогноз последующего развития событий”, — отмечает Ю.Б. Кашлев[102]. К сотрудникам дипломатических ведомств предъявляются новые, более высокие требования, которые связаны как более быстрым темпом жизни, большим объемом нужной и доступной информации, так и непосредственно с использованием новых технологий. Как отмечают специалисты, “в отличие от других форм внешнего опосредствования применение компьютерных средств при подготовке и реализации принятия решений требует перестройки интеллектуальных действий человека во внутреннем плане”[103], например, от пользователя требуется более точная формулировка его информационных запросов по сравнению с “традиционным” поиском в книгах и документах.

Информационные технологии в этом случае выступают не только как ответ на все возрастающий темп международной жизни, но и как самостоятельный вызов, требующий перестройки методов работы как каждого отдельного сотрудника, так и организации в целом. Как отмечают некоторые авторы, “внедрение новых технологий и методов управления информацией потребует постепенной, но серьезной перестройки структуры

---

[98] ***Беляев И.П., Трофимов Е.А.*** Системы поддержки принятия решений. Часть 1. Информационные системы поддержки принятия решений: Обзоры по электронной технике. Сер. 9. Экономика и системы управления. — М., ЦНИИ "Электроника", 1990. С. 43.

[99] ***Ушаков И.А.*** Предисловие к ***Саати Т.*** Ук. соч. С. 4.

[100] см. ***Гришин А. В., Никольский Н. М.*** Системный анализ и диалог с ЭВМ…, с. 93; ***Николаев Д.*** Информация в системе международных отношений. (Организация и функционирование информационных органов внешнеполитического механизма США). М.: Международные отношения, 1978. С. 135-136; США: организационные проблемы управления. М.: Мысль, 1976. С. 59; Reinventing Diplomacy in the Information Age. P. 37 и др.

[101] Diplomacy for the 21st Century. Information Technology Goals for the First Five Years. Building the New Information Organization. Office of Information Resource Management, U.S. Department of State. December 31, 1998. Chapter 4. (http://www.state.gov/www/dept/irm/98goals/chpt_4.html).

[102] ***Кашлев Ю.Б.*** Ук. соч.

[103] ***Беляев И.П., Трофимов Е.А.*** Системы поддержки принятия решений. Часть 2. Интеллектуальные системы поддержки принятия решений. С. 32.

дипломатических ведомств и того, как они выполняют свои функции… Традиционная иерархическая организация дипломатической службы, состоящая из центрального аппарата и миссий, должна постепенно трансформироваться в интегрированную систему. Роль каждого из участников в этой системе… должна определяться его возможным вкладом в определенный вид деятельности, а не иерархической позицией"[104]. Такая трансформация деятельности внешнеполитических органов (выражающаяся, в частности, в падении значения иерархии) является, с одной стороны, необходимым условием эффективного внедрения ИТ, а с другой — объективным процессом, связанным с развитием коммуникаций. Как свидетельствует американский исследователь С. Шварцстайн, расширение использования электронной почты и других новых технологий, в частности, в госдепартаменте США приводит к "сглаживанию" иерархии. "Неформальные" структуры возникают параллельно со старыми, устоявшимися "формальными"[105].

С точки зрения некоторых авторов, одной из основных задач на сегодня является улучшение системы принятия решений, в том числе с помощью компьютеров, с тем чтобы информация играла в этом процессе более важную роль. Одним из путей добиться этого может стать предоставление ЛПР всей необходимой информации в нужном объеме и в нужный момент (в том числе с широким использованием новых технологий), тогда игнорирование информации само по себе будет решением[106]. Вопрос о том, будет ли выполнена эта задача, возможность успешного осуществления которой серьезно ограничена не только организационными структурами, но и человеческой природой, остается открытым.

Подведем итог. Вопреки мнению некоторых политиков и обывателей, развитие коммуникаций и ИТ отнюдь не уменьшает значения профессии дипломата, а напротив, предъявляет к ней новые, более высокие требования. "Человеческий фактор" остается центральным в дипломатии, но использование современных информационных технологий постепенно превращается в обязательное условие эффективного труда сотрудников внешнеполитических органов. Возможности использования новых технологий разнообразны: от привычной большинству из нас электронной почты, получения информации из Интернета, пользования электронными каталогами и базами данных до сложных программ поддержки подготовки и принятия решений и внешнеполитического прогнозирования. Следует подчеркнуть, что даже самые простые и привычные из них вносят не только количественные, но и качественные перемены в процесс формулирования и осуществления внешней политики. Некоторые из новых технологий в перспективе способны изменить даже те отрасли внешнеполитической деятельности, которые традиционно считались исключительной прерогативой человека, например, переговоры и принятие решений.

Однако нельзя забывать, что какие бы "умные" новые технологии ни использовались, окончательное решение всегда остается за человеком. Только человек, помимо соображений оптимальности, выгодности обладает "чувством ситуации", творческим подходом, может принять во внимание моральные соображения. Поэтому несмотря на расширение использования ИТ, роль человека, принимающего решения, возрастает, особенно в современных условиях повышения цены за неправильное решение. Одновременно с возрастанием требований к сотрудникам внешнеполитических ведомств, с необходимостью определенной перестройки их деятельности во внутреннем плане, немаловажное значение имеет и перестройка деятельности всего ведомства в целом, в частности, должна измениться роль иерархии и возрасти роль информации в процессе принятия решения. Хотя подобные перемены в определенном смысле являются объективными, обусловленными внедрением в работу новых технологий, они же одновременно являются и условием эффективного использования ИТ, и от того, насколько необходимость таких реформ будет осознана как

---

[104] ***Jovan Kurbalija***. Op. cit.
[105] ***Schwartzstein S***. The Impact of Information Revolution on International Relations. IPTS Report, Vol 06: July 1996. (http://www.jrc.es/pages/iptsreport/vol06/english/art-it2.htm).
[106] ***Jovan Kurbalija***. Op. cit.

руководством внешнеполитических органов, так и каждым из их сотрудников, будет во многом зависеть направление дальнейшей эволюции как использования ИТ в этих ведомствах, так и самих ведомств.

**Источник:** http://www.auditorium.ru (05.05.2005)