

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский Нижегородский государственный университет
им. Н.И. Лобачевского» (ННГУ)

Институт международных отношений и мировой истории (ИМОМИ)

А.Е. Белянцев, В.А. Берендеев, И.В. Шамин

**НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
В МИРОВОЙ ПОЛИТИКЕ**

Учебно-методическое пособие

Рекомендовано методической комиссией
Института международных отношений и мировой истории
для студентов ННГУ, обучающихся по направлениям подготовки
41.03.05 «Международные отношения» и 41.03.04 «Политология»

Нижний Новгород
2019

УДК 327
ББК Ф4(0)я73
Б 44

Б 44 Белянцев, А.Е. Новые информационные технологии в мировой политике: учебно-методическое пособие [Электронный ресурс] / А.Е. Белянцев, В.А. Берендеев, И.В. Шамин. – Нижний Новгород: Изд-во ННГУ, 2019. – 63 с.

Рецензент: к. и. н., доцент **Ф.А. Дорофеев**

Данное учебно-методическое пособие предназначено для бакалавров, которые обучаются по направлениям «Международные отношения» и «Политология». Указанная работа может использоваться в процессе преподавания таких учебных дисциплин, как «История международных отношений» и «Основы международной и национальной безопасности», входящих в основную образовательную бакалаврскую программу направления «Международные отношения». Кроме того, пособие рекомендуется для бакалавров-политологов, изучающих учебные дисциплины «Политическая география мира», «Философия власти» и «ИКТ в современных политических процессах».

Ответственный за выпуск: председатель методической комиссии ИМОМИ ННГУ
к. и. н., доцент Бушуева С.В.

УДК 327
ББК Ф4(0)я73

© Национальный исследовательский
Нижегородский государственный университет
им. Н.И. Лобачевского, 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
ГЛАВА 1. Информационное «измерение» международной безопасности и проблемы конвергенции новейших технологий. Международно-правовое регулирование развития и внедрения современных технологий	6
1.1. Международная безопасность в условиях глобальной информационной революции.....	6
1.2. ТНК в глобальном информационном пространстве: новые вызовы и угрозы международной безопасности.....	14
1.3. NBIC-технологии как сфера международного взаимодействия.....	20
1.4. Вопросы для самоконтроля.....	28
ГЛАВА 2. Политические коммуникации и проблемы трансформации традиционных СМИ в глобальном интернет-пространстве	29
2.1. Масс-медийные эффекты глобальной информатизации.....	29
2.2. Интернет-пространство как фактор модернизации институтов гражданского общества.....	34
2.3. Интернет-коммуникации как средство развития и укрепления русскоязычной диаспоры.....	38
2.4. Вопросы для самоконтроля.....	40
ГЛАВА 3. Некоторые особенности современной информационной политики РФ	41
3.1. Технологии информационного общества как основа российской модернизации....	41
3.2. Информационная безопасность как важнейший фактор государственной информационной политики Российской Федерации.....	47
3.3. Вопросы для самоконтроля.....	54
ЗАКЛЮЧЕНИЕ	55
РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА	56
ТЕМЫ РЕФЕРАТОВ	61

ВВЕДЕНИЕ

Основной целью данного учебно-методического пособия является рассмотрение механизма влияния новейших информационно-коммуникационных технологий на современные международно-политические процессы, а также на формирование концептуального содержания определенных составляющих системы национальной безопасности РФ в условиях постбиполярного мира.

Представленный труд был подготовлен авторами на основе обобщения результатов исследований, проведенных отечественными и зарубежными специалистами по данной тематике в последнее время.

Данное учебно-методическое пособие предназначено для бакалавров, которые обучаются по направлениям «Международные отношения» и «Политология». Указанная работа может использоваться в процессе преподавания таких учебных дисциплин, как «История международных отношений» и «Основы международной и национальной безопасности», входящих в основную образовательную бакалаврскую программу направления «Международные отношения». Кроме того, пособие рекомендуется для бакалавров-политологов, изучающих учебные дисциплины «Политическая география мира», «Философия власти» и «ИКТ в современных политических процессах».

В Главе 1 в Разделах 1.1. (Международная безопасность в условиях глобальной информационной революции) и 1.2. (ТНК в глобальном информационном пространстве: новые вызовы и угрозы международной безопасности) рассмотрены проблемы влияния информационной революции и новейших ИКТ на мировой политический процесс, в частности, на акторов мировой политики (в основном таких как государства и ТНК), на взаимодействие между ними, на изменение форм международных конфликтов, а также на международную безопасность и возрастание интегрирующей роли ее информационной составляющей в системе глобальной безопасности. Также рассмотрены действия мирового сообщества по созданию международно-правового режима, регулирующего процессы глобальной информатизации.

Кроме того, в Разделе 1.3. (NBIC-технологии как сфера международного взаимодействия) проанализированы основные проблемы и направления международного сотрудничества в сфере управления рисками NBIC-конвергенции (конвергенция нанотехнологий, биотехнологий, информационных технологий и когнитивных технологий). Исследована деятельность международных организаций по регулированию и регламентации процесса развития новейших технологий и указано на необходимость эффективного международного взаимодействия в глобальном масштабе с целью контроля NBIC-процесса.

В Главе 2 исследованы процессы политической коммуникации и проблемы трансформации традиционных СМИ в глобальном интернет-пространстве.

Раздел 2.1. (Масс-медийные эффекты глобальной информатизации) посвящен особенностям функционирования современных СМИ в условиях глобализации и информационной революции. Проанализированы некоторые важные эффекты и характерные особенности активности СМИ как основного инструмента политической коммуникации в глобальном информационном пространстве. В заключении сделан вывод о возрастающем влиянии глобальных СМИ на современный мировой политический процесс.

В Разделе 2.2. (Интернет-пространство как фактор модернизации институтов гражданского общества) исследована деятельность институтов гражданского общества в российском сегменте Интернет-пространства. Проанализированы основные особенности активности в сети российских НКО, а так же новых субъектов гражданского общества – сетевых сообществ. Рассмотрено применение Интернет-технологий указанными

структурами с целью повышения эффективности гражданской активности. Сделан вывод о значительном модернизационном потенциале сети Интернет для институтов гражданского общества в современной России.

Раздел 2.3. (Интернет-коммуникации как средство развития и укрепления русскоязычной диаспоры) посвящен исследованию влияния сети Интернет на развитие, укрепление и эффективность диаспоральных связей. Проанализированы основные направления деятельности российской диаспоры (в качестве структуры гражданского общества) в Интернет-пространстве. Сделан вывод о возможности управления диаспорой, которую предоставляет Интернет, а также использовании ее для политического лоббизма в значимых для России странах.

В Главе 3 данного учебного пособия рассмотрены некоторые особенности современной информационной политики РФ.

Раздел 3.1. (Технологии информационного общества как основа российской модернизации) освещает основные направления информационной политики Российской Федерации и государственные инициативы по становлению информационного общества в контексте современных модернизационных процессов. Основное внимание уделено анализу источниковой базы информационной политики России, рассмотрены особенности российской модернизации в плане внедрения информационно-коммуникационных технологий в важнейшие сферы жизнедеятельности государства.

В Разделе 3.2. (Информационная безопасность как важнейший фактор государственной информационной политики Российской Федерации) исследованы основные направления информационной политики РФ и государственные инициативы по становлению информационного общества в контексте проблемы обеспечения информационной безопасности. Основное внимание уделено анализу документов РФ в сфере обеспечения информационной безопасности. Кроме того, рассмотрена деятельность России в рамках международных организаций в области информационной безопасности и нормативно-правового регулирования развития информационно-коммуникационных технологий.

В конце каждой главы учебного пособия приводятся вопросы для самоконтроля. Текст пособия завершается списком рекомендуемой литературы, а также списком тем рефератов в рамках указанной проблематики.

ГЛАВА 1. Информационное «измерение» международной безопасности и проблемы конвергенции новейших технологий. Международно-правовое регулирование развития и внедрения современных технологий

1.1. Международная безопасность в условиях глобальной информационной революции

Современные исследователи, рассматривающие теорию рисков и чрезвычайных ситуаций с точки зрения нелинейной динамики, утверждают, что для обеспечения безопасности в настоящих условиях необходимо внимательно следить за изменениями системных свойств нашего мира.

На рубеже столетий становится ясно, что наряду с огромными техническими достижениями и радикальными геополитическими переменами главным итогом уходящей эпохи явилось изменение системных свойств мира. У сложной системы как у целого могут появиться свойства, которыми не обладают ее части. В нынешнем быстро развивающемся мире создаются и уничтожаются сотни тысяч причинно-следственных отношений (длинная цепь которых может привести к тому, что система начинает вести себя парадоксальным образом), а с ними связаны и новые ресурсы развития, и новые риски. Появились новые методы борьбы, новые области соперничества, новые угрозы безопасности.

Новизну ситуации можно проиллюстрировать следующими примерами.

Если на заре истории главной ареной соперничества была суша, то со временем противоборство охватило море, глубины океана, воздух, космос. В XXI в., как полагают многие эксперты, главной ареной станет глобальное информационное пространство (киберпространство). Нынешние информационные технологии позволяют разрушить конкурирующее государство без единого выстрела.

Наполеон считал, что для того чтобы начать войну, ему надо убедить всех маршалов, три четверти генералов, половину офицеров, а солдаты и так пойдут. Системы управления, созданные в XX в., позволяют начать боевые действия, исходя из решения гораздо более узкого круга лиц. С другой стороны, появился слой людей, не относящихся к структурам власти, локальные действия которых могут причинить (или предотвратить) глобальный ущерб, исчисляемый миллиардами долларов. Это операторы атомных станций, командиры ядерных ракетносцев, руководители ряда финансовых структур. Их психологические установки, шкала ценностей, квалификация стали стратегическим ресурсом государства.

Опыт создания систем вооружений и организационных структур показывает, что не удается создать объекты, лишенные «ахиллесовой пяты». Это означает появление новых «экологических ниш» для террористов и др. акторов, готовых «играть не по правилам».

Наиболее серьезные угрозы часто находятся на системном уровне. Можно ценой больших затрат повысить надежность отдельных элементов, структур, однако, как правило, это не повышает безопасность в целом. Ответ на возможную угрозу также должен быть комплексным и системным.

Исследователи, работающие в рамках мировой политики, исходят из того, что за последние десятилетия политический мир стал более сложным по различным параметрам.

К важнейшим факторам жизни современного мирового сообщества можно отнести активно развивающиеся и влияющие на все сферы деятельности человечества процессы глобализации. Под глобализацией понимается процесс формирования единого общемирового финансово-информационного пространства. Это своего рода высшая стадия интеграции мирохозяйственных связей, информационной, экономической, технологической и культурной взаимозависимости современных государств и народов.

Поэтому в мировой политике усиливается значение экономической и информационной составляющих.

Процессы глобализации уменьшают власть национальных правительств (не обязательно государства как совокупности органов управления) внутри страны и на международной арене. Правительства все меньше могут управлять «своими» корпорациями. Транснациональные субъекты, неправительственные организации, все более международные СМИ затрудняют навязывание «своей» идеологии.

Вместе с крахом блоковой системы, ослаблением ООН, ОБСЕ, других организаций, связанных с прежней международной системой, падает ее общая управляемость, повышается уровень непредсказуемости и хаотичности.

Одновременно в связи с процессами глобализации и информационной революции происходит неинституционализируемая демократизация международных отношений. На мировой арене наряду с государствами все более активно действуют нетрадиционные акторы: ТНК, СМИ, группы давления, неправительственные организации, «интеллектуальные моды», различного рода движения, внутривластные регионы, межгосударственные организации и другие. Они оказывают растущее влияние на политические тенденции мирового развития. Эти «действующие лица» крайне многочисленны, разнородны, их влияние неоднозначно и порой трудно «просчитываемо».

Таким образом, мировая политическая система в процессе глобализации имеет тенденцию к усложнению, становится нелинейной, многомерной и многофакторной, а значит (в силу вышесказанного), у нее появляются новые системные свойства, с которыми связаны как новые ресурсы глобального развития, так и новые угрозы глобальной безопасности.

При исследовании принципиально нового информационного «измерения» современной системы международной безопасности предполагается выяснить:

- во-первых, как глобализация меняет представление о безопасности;
- во-вторых, каковы последствия информационной революции для сложившейся в мире системы безопасности.

Известный американский политолог, специалист в области теории безопасности М. Интрилигатор утверждает, что в результате глобальных нестабильностей и взаимозависимостей традиционные методы обеспечения безопасности становятся все менее подходящими, поэтому мировое сообщество должно выработать новые механизмы безопасности.

В современной ситуации необходимо трактовать безопасность исходя из глобальной, а не национальной или даже международной перспективы. Таким образом, традиционные концепции национальной и международной безопасности должны быть заменены новейшей концепцией глобальной безопасности, определяемой как отсутствие или избежание угроз жизненным интересам планеты. Безопасность достигается в современном мире не за счет другого государства, а одновременно с безопасностью других причастных государств. То есть повышение безопасности других не ослабляет ничью собственную безопасность. Содержание и сущность безопасности в процессе глобализации расширяются далеко за пределы традиционного военного измерения. Глобальная безопасность должна охватывать взаимосвязанные военные, политические, экономические, экологические и др. угрозы жизненным интересам планеты, т.е. возрастает роль невоенных компонентов. Даже в рамках традиционного более узкого определения безопасности, включающего предотвращение военных угроз жизненным интересам суверенного государства или группы объединенных государств, существуют более широкие проблемы глобальной безопасности.

Большинство современных ученых, исследующих мировой политический процесс (МПП), сходятся во мнении, что глобализация связана, прежде всего, с информационной революцией, т.е. качественно новым этапом развития средств связи и информации. Как отметил политический комментатор «Нью-Йорк Тайме» Т. Фридман, если основной

вопрос эпохи холодной войны заключался в количестве боеголовок, которыми располагала каждая сторона, то в постбиполярном мире главное – это быстрое действие компьютеров. Под МПП обычно понимается комплекс взаимосвязанных и взаимообусловленных политических процессов, протекающих на мировой арене в отдельных странах, регионах и в масштабе планеты как совокупная деятельность социальных общностей и институтов, организаций, групп и отдельных лиц, преследующих соответствующие политические цели.

Оценивая последствия информационной революции, рассматриваемой как распространение новых информационных технологий в глобальном масштабе, ее влияние на три составляющие МПП (субъекты, т.е. мировое сообщество; содержательную сторону, т.е. международные отношения, и безопасность), исследователи выделяют в основном следующие международно-значимые результаты этого феномена:

- децентрализация, прозрачность государственных границ, плюрализм;
- появление новых акторов (структур и субъектов глобального информационного пространства), действующих в международном масштабе;
- формирование сетевой, а не иерархической структуры сообществ;
- возрастание роли информационной компоненты безопасности;
- изменение природы международных конфликтов и подходов к их урегулированию.

Стремительное развитие за последние полвека информационно-коммуникационных технологий, которые непосредственным образом влияют на экономический, технологический и культурный прогресс человечества, формируют новую социально-политическую структуру «информационного общества», усиливают тенденцию к всеобщей взаимосвязи, взаимозависимости и взаимопроникновению в глобальном масштабе, дает основание говорить о таком феномене, как информационная революция, сравнимая по возможным последствиям с индустриальной революцией.

С начала 60-х гг. XX в. соединение воедино и совершенствование средств и каналов передачи информации, создание распределенных компьютерных сетей, электронных баз данных привело на пороге третьего тысячелетия к возникновению глобального информационного пространства в качестве инфраструктуры современного постиндустриального общества:

- в политической сфере все большее значение приобретают не силовые, а информационные факторы;
- в экономике происходит включение информационной продукции в систему товарных отношений, появилось множество коммерческих структур – производителей и потребителей информации, средств информатизации и защиты информации;
- растет зависимость экономического потенциала от уровня развития информационной инфраструктуры, а также потенциальная уязвимость экономики по отношению к информационным воздействиям;
- в информационной сфере произошел качественный скачок в процессах управления на всех его уровнях: от межгосударственных образований до отдельных фирм и банков, который обусловлен интенсивным развитием информационных технологий, дающих самые широкие возможности по совершенствованию и повышению эффективности управления.

Глубина этих процессов определяется не только воздействием каждой отдельной технологии, но и их взаимодействием, взаимоусилением.

Таким образом, формирование единого мирового информационного пространства превращается в глобальный фактор развития, определяет основные направления общественного прогресса, а сама информация становится важнейшим стратегическим ресурсом государств.

Глобализация информационных систем, охватывающих территории не только отдельных государств, но и целые континенты, условия легкого доступа к ним любого

человека создают совершенно новую ситуацию в области информационной безопасности.

С одной стороны, распределенные телекоммуникационные сети позволяют быстро и адекватно реагировать в режиме реального времени на любой «входной сигнал», будь то техногенная катастрофа, стихийное бедствие или военная угроза; осуществлять глобальное электронное управление и контроль через спутниковые системы как военного (MILSTAR), так и гражданского (COSPAS/SARSAT) назначения, а также высокоскоростную передачу информации через спутники связи. В этих случаях использование информационных технологий позволяет мировому сообществу своевременно предупреждать и стабилизировать конфликтные и чрезвычайные ситуации, быстро ликвидировать последствия стихийных бедствий и катастроф.

С другой стороны, в условиях такой взаимосвязи мира возникают угрозы безопасности на уровне информационного «измерения».

Следует отметить, что проблема обеспечения информационной безопасности в мире раньше не только не выдвигалась, но и фактически игнорировалась. Только сейчас мировое сообщество начинает серьезно и ответственно подходить к этой проблеме.

Под информационной безопасностью понимается состояние защищенности информационной среды, обеспечивающее ее формирование и развитие в интересах определенных структур. Информационная среда – это совокупность информационных ресурсов, система формирования, распространения и использования информации, информационной инфраструктуры. Угроза информационной безопасности – фактор или совокупность факторов, создающих опасность функционированию и развитию информационной среды.

На рубеже веков в мире сложилась многомерная структура международной безопасности, включающая в себя различные многосторонние институты и организации, действующие в рамках международного права; военно-стратегические альянсы; экономические союзы; региональные объединения и т.д., которая в огромной степени интегрирована в единое мировое информационное пространство. В рамках последнего производится накопление, обработка, хранение и обмен информацией между субъектами этого пространства — людьми, организациями, государствами. То есть в настоящее время вне глобальной «виртуальной территории» невозможно нормальное функционирование и эффективное управление всеми составляющими безопасности. Это обусловлено тем, что информационное пространство вбирает в себя одновременно экономическое, финансовое, масс-медиа, культурное, военное пространства настолько, насколько последние пронизаны телекоммуникациями. Совершенно естественно, что такая распределенная многофакторная система может быть подвержена специфическим угрозам.

Таким образом, современный мир находится в фундаментальной зависимости от нормального, бесперебойного функционирования информационной инфраструктуры. Происходит процесс лавинообразного повсеместного внедрения новейших информационных, телекоммуникационных и кибернетических технологий. Наряду с последними быстрое распространение локальных и глобальных сетей создает принципиально новое качество трансграничного информационного обмена. Все это самым непосредственным образом влияет на политику, экономику и безопасность.

Информационно-технологическая революция наряду с очевидными благами, которые она уже дала человечеству, и еще большими, ожидаемыми в будущем, одновременно создает принципиально новые угрозы использования достижений научно-технической мысли в этой области в целях, не совместимых с задачами поддержания международного мира, стабильности и безопасности, соблюдения принципов отказа от применения силы, невмешательства во внутренние дела других государств, уважения прав и свобод человека. Очевидно, что угрозы информационно-технологического характера явятся серьезным вызовом международной безопасности в XXI в. и существенно дополняют повестку дня процесса контроля за наиболее опасными видами вооружений и военной деятельности в мире.

Перечислим основные виды этих угроз:

1. Появление и стремительное распространение так называемых «метатехнологий», создающих возможность контроля над потребителем со стороны их разработчика. Специфика этого типа технологий в том, что сам факт их применения делает для использующей их стороны принципиально невозможной всякую серьезную конкуренцию с разработчиком этих технологий. Например, сетевой компьютер, рассредоточение памяти которого в сети дает разработчику доступ ко всей информации пользователя и позволяет первому вмешиваться в деятельность последнего или даже управлять ей (принцип внешнего управления включенного в сеть компьютера уже реализован); современные технологии связи, позволяющие перехватывать все телефонные сообщения на территории всего мира; в ближайшее время станет возможна полная компьютерная обработка всего объема этих сообщений и перехват всех сообщений в сети Интернет; а также различные организационные технологии, в т.ч. технологии управления, среди которых есть конструктивные для одной стороны и разрушительные для другой (элите противника под видом «новых» навязываются технологии управления, социально-политические и иные концепции развития, порождающие неразрешимые конфликты, создающие внутривнутриполитический хаос).

2. «Электронно-цифровой разрыв», т.е. возникновение элиты, обладающей неограниченным доступом к информации и коммуникационным сетям как на внутривнутригосударственном, так и на международном уровнях, использующей преимущество владения базами данных и связью в своих узких групповых целях и осуществляющей селективное распределение информации. В результате резко возрастают возможности манипулирования общественным мнением, базирующиеся на разных уровнях доступа отдельных людей, социальных групп, государств и т.д. к информации.

3. Информатизационная милитаризация, компьютерная преступность и терроризм.

Возможность использования колоссального потенциала информационно-кибернетических технологий в интересах обеспечения военно-политического превосходства, силового противоборства, шантажа меняет представление о вооруженных конфликтах, тактике и стратегии ведения боевых действий, открывает качественно новые направления гонки вооружений.

Особенность процесса информатизационной милитаризации заключается в том, что она происходит через конвергенцию гражданских и военных технологий, то есть они первоначально появляются и главным образом задействованы в гражданском секторе и лишь потом или на время переходят в военный.

Информационные технологии создали предпосылки для возникновения принципиально новой среды ведения боевых действий — киберпространства как части общего геостратегического ландшафта, а также появления информационного оружия. В связи с этим вооруженные конфликты все более приобретают характер информационных войн (т.е. акций, направленных на достижение контроля над информацией путем воздействия на информацию противника, его информационные процессы и информационные системы, а также на оборону собственной информации, информационных систем и процессов), которые имеют многомерный характер и могут одновременно вестись на различных фронтах и уровнях.

Информационная война выходит за рамки военного измерения. Она гораздо шире, чем боевые действия в области управления и контроля. В основном набор целей для информационной войны не будет набором военных целей. «Информационная война — электронный конфликт, в котором информация является стратегическим активом, достойным завоевания или уничтожения. Компьютеры и другие коммуникационные и информационные системы будут являться целями для первого удара и одновременно оружием в новой войне».

В широкой перспективе информационная война ведется во многих измерениях. Она является государственной стратегией, которая задействует все рычаги национальной

мощи для создания преимуществ на стратегическом уровне. Она является больше чем просто применением информационных технологий для увеличения эффективности современных инструментов войны. Она представляет собой действия, необходимые для того, чтобы парализовать не только системы военного управления и контроля противника, но и его политическую и финансовую системы.

Основными формами информационной войны являются (классификация дана М. Либики):

✓ Командно-управленческая война, которая нацелена на каналы связи между командованием и исполнителями. Перерезая «шею» (каналы связи) нападающий изолирует «голову» от «туловища». Кстати, Интернет родился как оборонный вариант этой войны («рассредоточенная шея»).

✓ Разведывательная война – сбор важной в военном отношении информации (как нападение) и защита собственной.

✓ Электронная война – направлена против средств электронных коммуникаций, радиосвязи, радаров, компьютерных сетей. Ее важный раздел — криптография (шифровка-расшифровка электронной информации). Сюда же входит и кибервойна (компьютерный терроризм), которая подразумевает диверсионные действия против гражданских объектов противника, такие, как тотальный паралич сетей, перебой связи, введение случайных ошибок в пересылку данных, тайный мониторинг сетей, несанкционированный доступ к закрытым данным. Оружием в этой войне являются компьютерные вирусы и др. программное обеспечение.

✓ Психологическая война – пропаганда, «промывание мозгов», информационная обработка населения. Эта форма войны имеет три составляющие – подрыв гражданского духа, деморализация вооруженных сил, дезориентация командования.

✓ Экономическая информационная война, т.е. нанесение ущерба экономической (производственной, финансовой, коммерческой и т.д.) сфере противника создание предпосылок для кризисных ситуаций.

Информационные атаки могут происходить на физическом, логическом и семантическом уровнях. На физическом уровне происходит разрушение аппаратных средств. На логическом уровне объект атаки – программные продукты. При семантической атаке компьютерная система работает совершенно правильно, но решения, которые она выдает – неверны. Семантическая атака направлена на «органы чувств» компьютерной системы, контролирующей какой-либо процесс с помощью сенсоров. Обмануть эти датчики или другие средства ввода – значит вывести систему из строя не нарушив в ней ничего.

В информационных войнах трансформируются многие понятия традиционной военной тактики, в частности такие, как «оборона», «наступление». В ходе локальных столкновений становится возможным обходиться без занятия территорий, не иметь дело с проблемой военнопленных, уменьшать потери в собственное живой силе, передоверяя инициативу в решении боевых задач безэкипажным средствам. Информационное нападение стирает грань начала военных действий размывает линию фронта, делает возможным нанесение ударов в точку сколь угодно удаленной от района непосредственного вооруженного противостояния.

Еще одна особенность информационных войн состоит в значительной трудности обнаружения и идентификации противника, которым может являться другое государство, международные террористические организации, экстремистские группы, преступные синдикаты, отдельные фанатики и хакеры, а также различные комбинации вышеперечисленных и др. субъектов информационного пространства, использующие современные глобальные сети для достижения своих целей.

К наиболее «критическим» (по отношению к информационному нападению) технологиям относятся информационные технологии, применяемые для обеспечения функционирования:

- органов государственного и военного управления;
- финансово-кредитных и банковских структур;
- систем связи и коммуникаций;
- систем управления различными видами транспорта, энергетики, экологически опасными производствами (ядерного, химического, биологического и др. профиля);
- систем предупреждения чрезвычайных ситуаций и ликвидации последствий стихийных бедствий и т.д.

Недооценка вопросов информационной безопасности этих систем может привести к непредсказуемым политическим, экономическим, экологическим и материальным последствиям, а также к значительным дополнительным человеческим жертвам.

Последствия возможных атак на «критическую инфраструктуру», которые могут быть предприняты из киберпространства, диктуют мировому сообществу необходимость уделять все большее внимание политическим, организационным и технологическим мерам защиты глобального информационного пространства.

Стратегия обеспечения устойчивости информационного пространства включает три основных элемента:

1. Повышенную защиту против возможных атак из киберпространства.
2. Способность обнаруживать признаки нападения.
3. Способность ответить на атаку и восстановить соответствующие функции после нападения.

К стратегии также относится защита сообщества специалистов по электронике, программному обеспечению и информатике.

Угроза возникновения подобных стратегий на национальном уровне ведет к тому, что в эпоху глобальной информатизации традиционные цели политической и экономической борьбы между государствами и их группировками постепенно заменяются задачами достижения мирового информационного превосходства.

Кроме того, простота и дешевизна доступа к средствам связи и передачи данных, космополитизм глобальных информационных сетей, с одной стороны, и уязвимость мировых информационных ресурсов, с другой, создают возможности использования информационно-кибернетических технологий в криминальных и террористических целях.

Необходимо подчеркнуть, что наиболее уязвимыми, с точки зрения последствий информатизационной милитаризации, а также компьютерных преступлений и терроризма, являются высокоразвитые в технологическом отношении государства, международные организации, транснациональные корпорации и финансовые институты, максимально вовлеченные в киберпространство.

Добиться реальных успехов в минимизации последствий всего комплекса перечисленных угроз глобальной безопасности возможно и целесообразно усилиями всего мирового сообщества, созданием международной системы информационной безопасности.

Опирающиеся на одну технологическую базу, принципиально новые угрозы режиму глобальной безопасности ставят проблему информационной безопасности в один ряд с такими проблемами, как нераспространение и уничтожение ядерного, ракетного и химического оружия, запрещение бактериологического оружия, борьба с международным терроризмом и распространением наркотиков и т.п. Эти проблемы невозможно решить усилиями одной или нескольких стран, на блоковой основе, в силу взаимозависимости информационных систем и неделимости мирового информационного пространства.

Объективно возникает потребность в международно-правовом регулировании мировых процессов гражданской и военной информатизации, разработке согласованной международной платформы в отношении информационной безопасности.

Важным шагом в данном направлении явилась резолюция 54/49 «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», принятая на 54 сессии Генеральной Ассамблеи ООН в 1999 г., по существу ставшая

формальным началом создания совершенно нового международно-правового режима, объектом которого будут информация, информационная технология и методы ее использования. В документе поставлен вопрос о целесообразности разработки международных принципов, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем и способствовали бы борьбе с информационным терроризмом и криминалом. Мировое сообщество признало международную информационную безопасность как глобальную проблему, как необходимое условие существования человечества в последующий век.

Следующим этапом на пути формирования нового мирового информационного порядка стал саммит «Большой восьмерки» в Японии в июле 2000 г. Главы государств и правительств, подписавшие Окинавскую хартию глобального информационного общества, признали, что информационно-коммуникационные технологии являются одним из наиболее важных факторов, влияющих на формирование общества XXI в. Революционное воздействие технологий касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. Они быстро становятся жизненно важным стимулом развития мировой экономики, а также дают возможность всем частным лицам, фирмам и сообществам, занимающимся предпринимательской деятельностью, более эффективно и творчески решать экономические и социальные проблемы.

В документе подчеркивается, что усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности киберпространства. Очевидно, что должно обеспечиваться осуществление эффективных мер в борьбе с преступностью в компьютерной сфере. Необходимо также найти эффективные политические решения актуальных проблем, как, например, попытки несанкционированного доступа и компьютерные вирусы. Будут привлекаться представители промышленности и других посредников для защиты важных информационных инфраструктур. Кроме того, на саммите в Окинаве премьер-министром Японии были выдвинуты предложения о комплексных совместных мерах в связи с наличием международного дисбаланса в распространении продукции цифровых технологий, где намечаются меры по интеграции развивающихся стран в глобальную информационную инфраструктуру и преодолению «цифрового разрыва» в Азиатско-Тихоокеанском регионе.

В этой связи также можно отметить многочисленные документы Европейского сообщества, посвященные различным аспектам информатизации экономики, информационной безопасности и выработке общих европейских позиций на международной телекоммуникационной арене.

В результате сейчас уже можно говорить о формировании международного информационного законодательства.

Таким образом, современная ситуация характеризуется появлением нового информационного «измерения» системы международной безопасности.

Глобализация трансформирует содержание мировой политики. Увеличивается роль проблем «мягкой безопасности», связанных прежде всего с информационной инфраструктурой и экономикой. Вопросы «жесткой безопасности» сохраняют вою значимость, все больше перемещаясь из плоскости военного противостояния ведущих государств в сферу соревнования в области высоких технологий и гонки вооружений.

Информационная сфера, являясь системообразующим фактором жизни мирового сообщества, активно влияет на состояние политической, экономической, военно-стратегической и других составляющих безопасности. Структура международной безопасности существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Информационные технологии становятся одним из наиболее важных факторов

управления современным миром, основным инструментом власти, влияющим на сложившуюся систему международных отношений и трансформирующим саму концепцию как национальной, так и международной безопасности.

Поэтому можно предположить, что система международной безопасности в XXI в. будет развиваться в двух тесно взаимосвязанных направлениях, первое из которых состоит в максимальном расширении позитивных возможностей, которые предоставляют информационные технологии мировому сообществу, а второе – в минимизации уязвимости и подверженности внешним угрозам глобального информационного пространства как инфраструктуры складывающегося постиндустриального общества. В условиях современной трансформации геостратегического ландшафта, расширяющегося за счет киберпространства, которое стало его неотъемлемой частью, данные направления являются приоритетными и создают возможности для дальнейшего изменения и развития всей структуры международной безопасности.

1.2. ТНК в глобальном информационном пространстве: новые вызовы и угрозы международной безопасности

К важнейшим факторам жизни современного мирового сообщества можно отнести активно развивающиеся и влияющие на все сферы деятельности человечества процессы глобализации и информационной революции. Поэтому в мировой политике усиливается значение экономической и информационной составляющих.

Одновременно происходит неинституционализованный демократизация международных отношений, т.е. на мировой арене наряду с государствами все более активно действуют нетрадиционные акторы (транснациональные корпорации (ТНК), СМИ, группы давления, неправительственные организации, внутривластные регионы, межгосударственные организации и т.п.), которые оказывают растущее влияние на политические тенденции мирового развития. Эти «действующие лица» крайне многочисленны, разнородны, их влияние неоднозначно и, порой трудно «просчитываемо».

Кроме того, соединение воедино и совершенствование средств и каналов передачи информации, создание распределенных компьютерных сетей, электронных баз данных привело на пороге XXI века к возникновению глобального информационного пространства (ГИП) в качестве инфраструктуры современного мира, который все более интегрируется в киберпространство и все более испытывает зависимость от нормального функционирования всех его составляющих. Возникновение ГИП радикально меняет не только экономическую, но и политическую жизнь планеты.

В настоящее время указанные акторы международных отношений в значительной степени внедряются в ГИП и активно действуют в рамках этой новой виртуальной территории в своих интересах.

Наиболее активными игроками на мировой экономической и политической арене выступают ТНК. Именно ТНК являются основным структурным элементом экономики большинства стран, ведущей силой их развития и повышения эффективности. Глобальные тенденции интернационализации производства и капитала, приватизации, стратегических альянсов и либерализации внешней торговли поставили ТНК в центр мирового экономического и политического развития.

ТНК, наравне с промышленно развитыми странами, широко проявляют себя в политике, экономике, в финансово-инвестиционной, информационной, научно-технической, военной, технологической, экологической сферах. Действия ТНК по характеру и формам проявления в мировой политике и экономике во многом совпадают с деятельностью государств, что позволяет экспертам если не отождествлять их, то, по

крайней мере, заявлять об идентичности действий и проявлений ТНК и государств в глобальной политике и экономике. В то же время ряд исследователей считают, что в перспективе ТНК смогут стать доминирующей силой мирового хозяйства, сменив национальные государства в качестве основных его объектов. Действия ТНК в ГИП во многом подтверждают указанные выше тенденции.

Анализируя деятельность современных ТНК в ГИП, можно прийти к выводу, что они являются, пожалуй, основными действующими лицами на мировой телекоммуникационной арене. Это обстоятельство имеет под собой фундаментальные основания.

Глобальный мир ТНК имеет существенно сетевую трансграничную структуру. Его формирование происходило одновременно с интенсивной сетевой информатизацией общества, развитие этих процессов носило взаимодополняющий характер.

Сетевые структуры обеспечивают глобализацию капитала и децентрализованную концентрацию производства и труда. Образуется всемирное информационно-финансовое пространство. ТНК входят в союзы с мегаполисами и образуют структурные узлы сетей. Возникает единое рыночно-информационное пространство, интегрированное в ГИП. Поэтому структуры ТНК естественным образом вписываются в ГИП. С одной стороны, развивая, строя и расширяя его, а с другой – максимально используя преимущества, которые оно им предоставляет. Что же касается ТНК, производящих информационный продукт или сетевых ТНК (например, владельцев ОТКС – открытых информационно-телекоммуникационных сетей, а так же транснациональных СМИ), то ГИП является для них жизненно важной инфраструктурой, просто позволяющей существовать и разворачивать свою деятельность.

При рассмотрении целого ряда проблем и вызовов «электронного века» сквозь призму деятельности ТНК, можно сделать вывод о неоднозначности их влияния на современную ситуацию в области международной безопасности, информационная компонента которой в значительной мере возрастает с ростом и расширением ГИП. Эта неоднозначность объясняется двойственной природой любой информационной технологии. Одну и ту же технологию обработки информации можно использовать как в положительном, так и в отрицательном (с точки зрения безопасности информационной системы) аспекте.

Проанализируем основные глобальные угрозы и вызовы в информационной сфере и деятельность ТНК в этой связи.

1) Многие исследователи выделяют проблему появления и стремительного распространения в глобальном масштабе так называемых информационных «метатехнологий», которые создают возможность полного контроля над потребителем, со стороны их разработчика. Специфика этого типа технологий в том, что сам факт их применения делает для использующей их стороны принципиально невозможной всякую серьезную конкуренцию с владельцем этих технологий. Например, сетевой компьютер, рассредоточение памяти которого в сети дает разработчику доступ ко всей информации пользователя и позволяет первому вмешиваться в деятельность последнего или даже управлять ей (принцип внешнего управления включенного в сеть компьютера уже реализован); современные технологии связи, позволяющие перехватывать все телефонные сообщения на территории всего мира (в ближайшее время станет, возможна полная компьютерная обработка всего объема этих сообщений и перехват всех сообщений в сети Интернет); технологии (в основном для СМИ) формирования массового сознания, а также различные организационные технологии, в т.ч. технологии управления, среди которых есть конструктивные для одной стороны и разрушительные для другой (элите противника под видом «новых» навязываются технологии управления, социально-политические и иные концепции развития, порождающие неразрешимые конфликты, создающие внутривнутриполитический хаос).

Естественно, что разработчиками такого рода технологий являются, в основном, ТНК, работающие в сфере производства информационного продукта (например, Microsoft, AOL-TimeWarner, CNN и др.).

С другой стороны, распространение информационных метатехнологий позволяет быстро и адекватно реагировать в режиме реального времени на любой «входной сигнал», будь то техногенная катастрофа, стихийное бедствие или военная угроза; осуществлять эффективное глобальное электронное управление и контроль через спутниковые системы как военного, так и гражданского назначения, а также высокоскоростную передачу информации через спутники связи, что создает возможности для своевременного предупреждения и стабилизации конфликтных и чрезвычайных ситуаций, скорейшей ликвидации последствий стихийных бедствий и катастроф. Так же информационные метатехнологии способствуют конкуренции, увеличивают доступность многих услуг для населения (через систему электронной торговли), повышают возможность получения образования, медицинских услуг, а системы электронного правительства позволяют наиболее полно учитывать общественное мнение, развивают демократические институты.

2) Неоднозначны также и последствия деятельности ТНК для ликвидации «электронно-цифрового разрыва».

С одной стороны, деятельность ТНК по распространению информационных технологий в развивающихся, в частности, странах имеет положительные последствия (см. выше) как для экономики, демократизации, так и для безопасности в целом.

С другой – появляется возможность возникновения элиты (в лице ТНК, в особенности), обладающей неограниченным доступом к информации и коммуникационным сетям, как на внутригосударственном, так и на международном уровнях, использующей преимущество владения базами данных и связью в своих узких групповых целях и осуществляющей селективное распределение информации. В результате резко возрастают возможности манипулирования общественным мнением, базирующиеся на разных уровнях доступа отдельных людей, социальных групп, государств и т.д. к информации.

3) Целый комплекс новых угроз и вызовов международной безопасности связан с процессами информатизационной милитаризации, компьютерной преступностью и терроризмом.

Особенность процесса информатизационной милитаризации заключается в том, что она происходит через конвергенцию гражданских и военных технологий, то есть они первоначально появляются и главным образом задействованы в гражданском секторе и лишь потом или на время переходят в военный.

Информационные технологии создали предпосылки для возникновения принципиально новой среды ведения боевых действий – киберпространства, как части общего геостратегического ландшафта, а также к появлению информационного оружия. В связи с этим вооруженные конфликты все более приобретают характер информационных войн (т.е. акций, направленные на достижение контроля над информацией, путем воздействия на информацию противника, его информационные процессы и информационные системы, а также на оборону собственной информации, информационных систем и процессов), которые имеют многомерный характер и могут одновременно вестись на различных фронтах и уровнях.

Информационная война выходит за рамки военного измерения. В основном набор целей для информационной войны не будет набором военных целей. Она является больше чем просто применением информационных технологий для увеличения эффективности современных инструментов войны и представляет собой действия, необходимые для того, чтобы парализовать не только системы военного управления и контроля противника, но и его политическую и финансовую системы. «Информационная война - электронный конфликт, в котором информация является стратегическим активом, достойным завоевания или уничтожения. Компьютеры и другие коммуникационные и

информационные системы будут являться целями для первого удара и одновременно оружием в новой войне».

К наиболее «критическим» (по отношению к информационному нападению) технологиям относятся информационные технологии, применяемые для обеспечения функционирования:

- органов государственного и военного управления;
- финансово-кредитных и банковских структур;
- систем связи и коммуникаций;
- систем управления различными видами транспорта, энергетики, экологически опасными производствами (ядерного, химического, биологического и др. профиля);
- систем предупреждения чрезвычайных ситуаций и ликвидации последствий стихийных бедствий и т.д.

Недооценка вопросов информационной безопасности этих систем может привести к непредсказуемым политическим, экономическим, экологическим и материальным последствиям, а также к значительным дополнительным человеческим жертвам.

Кроме того, простота и дешевизна доступа к средствам связи и передачи данных, космополитизм глобальных информационных сетей, с одной стороны, и уязвимость мировых информационных ресурсов, с другой, создают возможности использования информационно-кибернетических технологий в криминальных и террористических целях.

Необходимо подчеркнуть, что наиболее уязвимыми с точки зрения последствий информатизационной милитаризации, а также компьютерных преступлений и терроризма являются высокоразвитые в технологическом отношении государства, международные организации, ТНК и финансовые институты, максимально вовлеченные в киберпространство.

Анализируя вышесказанное, можно предположить, что у ТНК существуют две взаимно дополняющие друг друга стратегии поведения в ГИП, касающиеся процессов информационной милитаризации и компьютерного терроризма.

Первая – активная работа по созданию безопасного ГИП, разработка политических, организационных и технологических мер его защиты в целом, что диктуется возможными последствиями атак на «критическую инфраструктуру» (жизненно важную, в том числе, и для ТНК), которые могут быть предприняты, из киберпространства.

Стратегия обеспечения устойчивости информационного пространства включает три основных элемента:

1. повышенную защиту против возможных атак из «киберпространства»,
2. способность обнаруживать признаки нападения,
3. способность ответить на атаку и восстановить соответствующие функции после нападения.

Сюда также примыкает защита сообщества специалистов по электронике, программному обеспечению и информатике.

Добиться реальных успехов в минимизации последствий всего комплекса перечисленных угроз глобальной безопасности возможно и целесообразно усилиями всего мирового сообщества, созданием международной системы информационной безопасности. Важную роль в этом процессе играют ТНК.

Вторая стратегия – активное участие ТНК в информационном противоборстве, инфомационная экспансия, позволяющая получить преимущества для ведения бизнеса в глобальном масштабе. ТНК в качестве субъектов информационного противоборства, конкурируют в ГИП с государствами, образуют различные виртуальные коалиции, активно ведут разработки информационного оружия.

Остановимся более подробно на характеристике ТНК, как одного из основных субъектов информационного противоборства. Этот вид субъектов информационного противоборства обладает следующими характеристиками (признаками) субъектности:

- имеет, как правило, стабильные (постоянные) интересы в информационно-телекоммуникационном пространстве;
- участвует в формировании ГИП и частично контролирует национальные сегменты информационного пространства;
- создает в рамках своих структур или использует национальные структуры государств, интегрированных в контролируемое данным субъектом информационное и телекоммуникационное пространство, в функции и задачи которых входит ведение информационного противоборства;
- создает и использует собственный научно-технический потенциал и/или использует (стимулирует создание) потенциал стран, так или иначе интегрированных в сегмент информационного пространства, принадлежащего и/или контролируемого корпорацией, или принимающих участие в ее деятельности, для разработки и испытаний образцов и систем информационного оружия, средств его доставки и маскировки, принципов применения, а также приобретает при необходимости (тайно) данные средства у третьей стороны;
- разрабатывает и закрепляет на официальном уровне, в том числе в виде ведомственных нормативных актов, концептуальные и идеологические положения, обосновывающие необходимость участия в информационном противоборстве, определяющие основные принципы и формы участия в нем для данного субъекта.

Особую роль в информационной борьбе владельцев ОТКС и разработчиков сетевых технологий – сетевых информационных корпораций и корпораций-провайдеров, обеспечивающих циркуляцию жизненно важных потоков информации, можно охарактеризовать следующим образом.

В информационном обществе условия диктует тот, в чьих руках находятся информационные сети, ресурсы и технологии. Контроль за сетевыми ресурсами сосредоточен в руках провайдеров, обеспечивающих доступ в открытые телекоммуникационные сети для других компаний, организаций и частных лиц и гарантирующих стабильность работы с информационными потоками и сетевыми ресурсами. Деятельность провайдеров может подвергаться контролю и давлению как со стороны частных фирм и корпораций, так и органов власти тех государств, на территории которых находятся их сервера, представительства и иные активы. Однако в тех случаях, когда сетевые ресурсы компании-провайдера находятся на территориях нескольких государств, обеспечивая стабильную работу государственных органов власти и других организаций с различной формой собственности, вмешательство органов власти одного государства в работу такой компании может нанести ущерб политическим и экономическим интересам других государств, что, с одной стороны, может привести к нежелательным осложнениям во внешнеполитических отношениях, с другой,--- становится хорошей гарантией безопасности и стабильности для таких компаний, так как в случае нарушения их деятельности на защиту компании, обеспечивающей циркуляцию потоков информации, обязательно придут правительственные структуры и законы тех стран, которые заинтересованы в надежной работе этого канала обмена информацией и информационного воздействия. Такие условия существования крупных информационных компаний, контролирующих сети и потоки циркулирующей в них информации, во многом сходны с условиями деятельности банковской системы Швейцарии, которые обеспечили безопасность и неприкосновенность границ этой небольшой альпийской страны в течение двух мировых войн. Таким образом, компании, контролирующие открытые информационные сети и информационные потоки в них, все больше приобретают черты транснациональных государств-корпораций, интересы которых лежат на территориях различных стран с различными законами, традициями, геополитическим положением и государственным устройством.

Также можно прийти к выводу о том, что в ближайшем будущем в любом вооруженном конфликте будут задействованы силы и средства как минимум трех сторон--

- агрессора, жертвы агрессии и (одной или нескольких) корпораций, обеспечивающих бесперебойное функционирование ОТКС (являющихся полем деятельности сил специальных информационно-психологических операций государства-агрессора и государства-жертвы агрессии) и контролирующих циркулирующую в них информацию. Следует отметить, что, несмотря на то, что все три стороны, очевидно, являются активными участниками конфликта и имеют самое непосредственное к нему отношение, только две из них (агрессор и жертва) находятся в юридически оформленном и закрепленном состоянии войны, третья же сторона (компания-провайдер) придерживается нейтралитета. Учитывая, что без содействия (или хотя бы при невмешательстве) провайдера, контролирующего ОТКС, силы специальных информационно-психологических операций обеих сторон вряд ли добьются желаемых результатов, активная же позиция структур, контролирующих информационные сети, может стать решающей для обеспечения успешных действий наступающей или обороняющейся стороны.

Появление надгосударственных международных информационно-сетевых корпораций, располагающих сетевыми ресурсами, расположенными на территориях различных стран мира, может привести в случае проведения силами специальных информационно-психологических операций враждующих сторон активных боевых действий на каналах ОТКС и СМИ к нанесению по вооруженным силам, населению и коммуникациям противника ударов с территорий государств, не только являющихся нейтральными по отношению к этому конфликту (не имеющих в этом регионе своих интересов) и непосредственно не примыкающих территорией к театру военных действий, но и связанных с государствами-участниками конфликта дипломатическими соглашениями различного характера (внешнеполитическими и внешнеэкономическими, торговыми, социальными, культурными и др.). Нет сомнений, что внезапность таких ударов будет новым и достаточно важным фактором, способным повлиять на характер боевых действий в целом и, при определенной трактовке таких действий враждующими сторонами, может привести к расширению очага конфликта и вовлечению в конфликт новых участников.

При этом особую роль сетевых корпораций в информационно-психологической борьбе государств можно охарактеризовать следующим образом.

1. ТНК в информационном обществе обладают всеми признаками суверенного государства – территорией, определяемой ареалом распространения их сетевой инфраструктуры, стратегическими ресурсами (информацией и информационными потоками, циркулирующими в принадлежащих или подконтрольных им информационно-телекоммуникационных сетях), аналогом населения (штатом лояльных сотрудников и агентов влияния) и относительно полным суверенитетом, выражающимся в реальной возможности не только отстаивать собственные интересы на международном уровне с вовлечением в решение собственных политических вопросов субъектов международной политики, но и оказывать давление на субъекты международной политики, деятельность и состояние безопасности которых зависит от стабильного функционирования сетевой инфраструктуры, притока информационных и сетевых ресурсов и новых информационно-телекоммуникационных технологий).

2. Транснациональные сетевые корпорации в информационном обществе, разрабатывая новые информационные технологии, развивая принадлежащие им глобальные информационно-телекоммуникационные сети и контролируя циркулирующие по ним потоки, вообще говоря, не принадлежащей им информации, создают тот театр военных действий, на котором затем будут разворачиваться боевые действия между участниками информационно-психологического противоборства. Новые информационные и телекоммуникационные технологии дают враждующим сторонам тот арсенал сил и средств нападения и обороны, который затем и будет использован в информационно-психологическом конфликте. Таким образом, можно считать, что информационная война

ведется субъектами информационного противоборства в сфере, искусственно создаваемой человеком в результате разработки новых средств воздействия (информационных технологий) и средств доступа к уязвимым объектам нападения (сетевой инфраструктуры), т.е., фактически, в условиях и по законам, определяемым разработчиками и владельцами сетей и технологий.

На фоне прогрессирующих процессов информационной, психологической, экономической, культурной глобализации развивается процесс вытеснения традиционных государств информационными сверхкорпорациями. Следует ожидать появления в ближайшие 10–15 лет частных компаний, обладающих признаками суверенных государств: экстерриториальность; наличие собственных легитимных вооруженных сил; участие в международных организациях, предусматривающих членство только для суверенных субъектов. Параллельно с этим будут развиваться и государственные образования традиционного типа.

Одновременное развитие как государств традиционного типа, так и экстерриториальных сверхкорпораций будет протекать какое-то время без силовых конфликтов между ними. Традиционная государственность получит свое дальнейшее развитие в тех регионах, где частный бизнес недостаточно развит, чтобы сформировать внутри себя экстерриториальный субъект негосударственного типа (сверхкорпорацию) – в Латинской Америке, Юго-Восточной и Центральной Азии, Африке. В постиндустриальных регионах (Северная Америка и Европа), процессы взаимодействия государства и сверхкорпораций будут происходить на базе имеющихся правовых механизмов.

В этих условиях национальные ОТКС (и степень их развитости на территории государства) можно рассматривать как один из важнейших факторов информационной геополитики, определяющих геополитический ландшафт в информационно-психологическом пространстве современного общества. В информационной сфере информационно-телекоммуникационные сети и сетевая инфраструктура, в которых циркулируют потоки важнейшего стратегического ресурса информационного общества – информации, определяют масштабы информационного пространства государства и при оценке мощи государства и его геополитического потенциала вытесняют по своей значимости на второй план размеры и географические особенности территории, акватории и воздушного пространства государства, степень развитости и эффективности его наземных, воздушных и морских коммуникаций.

Таким образом, активная позиция в ГИП органична, естественна и жизненно необходима для ТНК, поскольку они являются сетевыми трансграничными организациями и используют, а также расширяют и формируют ГИП в качестве инфраструктуры, необходимой для своей успешной деятельности. Эта деятельность неоднозначна и имеет как положительные, так и отрицательные грани с позиции учета новых глобальных угроз и вызовов информационной эпохи.

1.3. NBIC-технологии как сфера международного взаимодействия

В настоящее время развитие науки и техники определяется ускоряющимся прогрессом в таких областях, как информационные технологии, биотехнологии, нанотехнологии и когнитивная наука. Эти технологии не развиваются в изоляции, а активно влияют друг на друга. Подобное явление взаимоусиления технологий получило название NBIC-конвергенции.

Развитие NBIC-технологий сильно меняет привычные представления о мире, в том числе – о природе базовых понятий, таких, как жизнь, человек, разум, природа. Результаты подобных трансформаций, когда изменению подвержены все аспекты жизни

человека и общества, трудно предсказуемы. Но можно ожидать, что изменения станут все более стремительными.

Поэтому в современной ситуации, характеризующейся процессом конвергенции технологий подход, связанный с глубоким осмыслением целей, долгосрочным планированием, многоуровневым регулированием и анализом последствий принимаемых решений в глобальном масштабе должен стать основой будущего развития цивилизации.

Как мир должен реагировать на технологии, сочетающие обещание колоссальных потенциальных выгод с угрозами, как физическими и явными, так духовными и весьма скрытыми? Ответ очевиден: нужно использовать силу государства, чтобы эти технологии регламентировать. А если их регламентация окажется не по силам любому отдельно взятому национальному государству, потребуется международное регулирующее законодательство. И надо начать конкретно продумывать, какие необходимо создать институты, чтобы отличать хорошие применения новейших технологий от плохих, и как заставить эти законы работать на национальном и международном уровнях.

Главная проблема заключается в неравномерном распределении био- и нанотехнологических ресурсов среди стран. Это может повторить ситуацию, сложившуюся в ядерной сфере с режимом нераспространения. Страны, отставшие по тем или причинам в развитии новых технологий, не будут стремиться к какому либо международному сотрудничеству по контролю и тем более ограничению использования комплекса новейших технологий. Современные глобальные средства коммуникации сделали доступными достижения науки широкому кругу людей. Активное участие негосударственных акторов в развитии и использовании современных технологий осложняет контроль. Это создает основу для социальных конфликтов на разных уровнях: локальном, региональном, международном. На каждом из этих уровней необходимо разрабатывать механизмы и институты управления рисками.

Кроме того, есть все основания полагать, что преимуществами применений новейших технологий воспользуются развитые, более богатые страны. Это также может привести к обострению противоречий и возникновению конфликтов между «победителями» и «побежденными». В этой связи особая нагрузка ложится на международные организации и институты, такие как Международная организация по стандартизации (ISO), ЮНЕСКО, Европейский Союз (ЕС), Организация экономического сотрудничества и развития (ОЭСР), которые начали разрабатывать новые стандарты и анализировать социально-политические и этические аспекты развития новейших технологий.

На государственном уровне регулирование комплекса конвергентных технологий осуществляется во многих странах мира. Так можно отметить развернутые стратегии инновационного технологического развития, реализуемые в США, Канаде, Японии и др. странах, а также на уровне ЕС (как в отдельных государствах, так и общеевропейские).

Процессы международного регулирования сферы конвергентных технологий, предотвращения соответствующих угроз и управления рисками развиваются в трех взаимосвязанных направлениях:

- поиск новых неклассических подходов к управлению рисками в условиях высокой степени неопределенности, характерной для NBIC-процесса;
- регулирование всего комплекса конвергентных технологий, включая выработку стратегий глобального технологического развития в рамках существующих международных институтов и организаций;
- создание новых международных институтов, регулирующих и регламентирующих развитие новейших технологий.

Принципиален тот факт, что поскольку угрозы и риски комплекса NBIC-технологий для человеческой цивилизации могут быть существенны и во многом пока непредсказуемы, нельзя рассчитывать, на то, что в процессе дальнейшего развития и самоорганизации естественным путем (без вмешательства государств и международных

институтов) будут выработаны соответствующие регламенты безопасного функционирования данного комплекса технологий. Такой подход эффективен и частично используется, например, при выработке регламентов информационной безопасности в компьютерных сетях, однако для регулирования NBIC-процесса, в силу указанных причин, он неприменим.

Поиск решений, позволяющих обществу эффективно функционировать в условиях постоянно нарастающих рисков техногенного характера и неопределенности сценариев его будущего развития, подстегиваемых NBIC-конвергенцией, является важнейшей задачей. К числу таких решений относится принцип предосторожности.

Применительно к технологиям, результаты развития которых непредсказуемы, в ситуациях, когда, ускорение вызываемых технологией процессов уже не оставляет времени на их коррекцию, необходимо исходить из того, что обоснованные возможности отрицательных последствий имеют преимущество перед не менее обоснованными возможностями положительных последствий.

С некоторыми модификациями принцип предосторожности был включен в декларацию конференции ООН по окружающей среде и развитию в Рио-де-Жанейро (1992 г.), а затем и в другие международно-правовые акты, связанные с охраной окружающей среды, биотехнологиями и генно-инженерной деятельностью. В дальнейшем он был введен в национальное законодательство ряда стран и правовые акты таких наднациональных образований, как ЕС. В европейских странах применение принципа предосторожности для регулирования развития конвергентных технологий во многом следует логике использования этого принципа для регулирования нанотехнологий.

Толкование принципу предосторожности было дано судом ЕС, который установил, что в случаях, когда наличие и объем опасности для здоровья человека неизвестны, институты ЕС могут вводить меры защиты, не дожидаясь точной информации о наличии и объеме угрозы. Т.е. принцип предосторожности служит обоснованием экстренных мер, принятых без опоры на достаточные научные обоснования. Принятие или непринятие таких мер – это политическое решение, относящееся к сфере управления рисками.

Потенциальные риски и угрозы био- и нано- технологий (как отдельно для каждой технологии, так и в комплексе, в соединении с ИКТ и когнитивными технологиями), связаны с новыми качествами и свойствами, которые проявляются у известных веществ в нанодиапазоне, а также новыми свойствами ГМО и трансгенных организмов и, тем более, активных гибридных нанобиоструктур. В настоящее время ведутся дискуссии относительно возможных последствий их применения для здоровья человека, состояния окружающей среды и безопасности. Причем эти последствия пока не удастся однозначно определить даже для современного поколения наноструктур и продуктов биотехнологий, не говоря уже о будущем.

Однако на данный момент существует общее понимание – риски развития конвергентных технологий настолько значительны для человечества и планеты, что требуется правовая защита от их последствий, даже если этим будет затронута свобода исследований.

Классификация рисков, на основании которой может приниматься решение об использовании принципа предосторожности, включает четыре вида рисков:

- известный риск. В данном случае последствия и воздействия, а также вероятность их наступления уже известны, и управление рисками заключается в установлении принятого уровня защиты;
- риск, не поддающийся количественной оценке, характеризуется тем, что, несмотря на наличие информации о возможных воздействиях или последствиях, отсутствует достоверная информация о связях между причинами возникновения рисков и наступлением неблагоприятных последствий, что делает невозможным рассчитать вероятность наступления вреда или причинения ущерба;

- гносеологическая неопределенность. К этой категории относятся риски, связанные с недостаточными научными знаниями и отсутствием единого мнения ученых о возможных последствиях, их опасности, вероятности их наступления;

- гипотетические риски – это риски, которые вообще не могут быть рассчитаны, так как научные знания в соответствующей области отсутствуют. Поэтому оценка рисков данном случае имеет характер предположений.

Принцип предосторожности возможно применить ко второй и третьей категориям рисков. В случае когда риски известны, применяется принцип ALARA (англ. – AsLowAsReasonablyAchievable), под которым понимается требование достичь минимально возможного уровня рисков или вредного воздействия. К четвертой группе рисков принцип предосторожности не может применяться, так как отсутствуют научные данные, на основании которых можно принять решение.

Применение принципа предосторожности характерно для ситуации неуверенности в отношении последствий в отличие от традиционного управления рисками, основывающегося на знаниях о величине возможного ущерба и вероятности его наступления. Политическая цель традиционного управления рисками – их минимизация и предупреждение нежелательных долгосрочных эффектов. Политическая цель управления рисками в ситуации неуверенности, – уменьшение неуверенности, представление как можно большего объема точной информации о рисках, собранной постепенно в ходе мониторинга, и возможное установление долгосрочных негативных последствий [4].

В связи с темой регулирования всего комплекса биотехнологий в глобальном масштабе можно выделить некоторые проблемы в деятельности международных организаций.

Одним из основополагающих документов, регулирующих биотехнологии на международном уровне, является Картахенский протокол по биологической безопасности (КПББ). Этот документ разрабатывался под эгидой ООН в рамках Программы объединенных наций по окружающей среде (UNEP) и был подписан более чем 130 странами 29 января 2000 г. в Монреале. Протокол служит международным гарантом для регулирования рынка генетически модифицированных продуктов (ГМП). Он охватывает круг проблем, связанных с группой сельхозтоваров, и не затрагивает фармацевтическую и иную продукцию (в этом заключается его главный недостаток). Неопределённость воздействия этих товаров на человека и является главной проблемой регулирования рынка ГМП, которая на международном уровне находится в компетенции ВТО, а на национальном – под контролем правительств.

Конвенция о запрещении разработки, производства и накопления запасов бактериологического (биологического) и токсинного оружия и об их уничтожении (КБТО, 1972 г.) определяет все работы по созданию токсичных агентов как преступление международного масштаба. Однако современный уровень биотехнологий позволяет создать биологическое оружие, которое невозможно идентифицировать и нейтрализовать, не располагая разработками высокого уровня. Эволюция биологического и химического оружия привела к созданию нового вида вооружений – так называемого генного оружия, которое базируется на последних достижениях молекулярной биологии по расшифровке генома человека. Простота технологии создания средств биотеррористической атаки позволяет сделать сам акт такой атаки непредсказуемым.

По мнению ряда экспертов, в современной ситуации существуют большие пробелы в области регулирования как агробиотехнологии, так и биотехнологии человека в особенности. Поэтому в рамках международного сотрудничества являются актуальными вопросы совершенствования уже существующих наднациональных институтов и создания новых, обладающих реальной властью по регулированию и регламентации биотехнологии на основаниях более широких, чем эффективность и безопасность, а также уставными полномочиями контроля над любыми исследованиями и разработками, финансируемых из любых источников.

В плане регулирования сферы нанотехнологий, а также прогнозирования результатов их развития можно отметить деятельность следующих международных организаций.

В 2004 г. на базе Центра биологических и экологических нанотехнологий Университета Райса (Rice University, USA) учрежден Международный Совет по нанотехнологиям (International Council on Nanotechnology, ICON) – организация, цель которой способствовать активному обмену информацией по вопросам оценки рисков нанотехнологий для здоровья человека и окружающей среды и таким образом содействовать уменьшению отрицательных последствий промышленных наноматериалов для общества. В октябре 2006 г. ICON выпущен обзорный доклад, в котором, в частности, говорилось о необходимости ограничения распространения информации по нанотехнологическим исследованиям в целях безопасности.

В 2008 г. учреждена международная нанотоксикологическая организация (International Alliance for NanoEHS Harmonization) призванной установить протоколы для воспроизводимого токсикологического тестирования наноматериалов на клетках и живых организмах.

На международном уровне разработаны и действуют документы, регламентирующие технические аспекты развития сферы nanoиндустрии.

Так, например, Международной организацией по стандартизации (International Organization for Standardization – ISO), приняты международные документы по стандартизации в сфере нанотехнологий, такие, как ISO/TR12885:2008 «Нанотехнологии. Правила техники безопасности, применяемые в профессиональной деятельности», ISO/TS27687:2008 «Нанотехнологии. Термины и определения нанообъектов. Наночастица, нановолокно и нанопластина», ISO/TS10867:2010 «Нанотехнологии. Определение характеристик одностенных углеродных нанотрубок с помощью инфракрасного фотолюминесцентного спектроскопа», ISO/TR11360:2010 «Нанотехнологии. Методология классификации наноматериалов», ISO29701:2010 «Нанотехнологии. Проверка на эндотоксин образцов наноматериалов в системах «ин витро». Испытания методом Limulusamebocytelysate (LAL)», ISO/TS80004-1:2010 «Нанотехнологии. Термины и определения. Часть 1. Основные термины», ISO/TS80004-3:2010 «Нанотехнологии. Термины и определения. Часть 3. Углеродные нанообъекты», IEC 62624:2009 «Методы измерений электрических свойств углеродных нанотрубок».

Кроме того, в рамках ISO принята «Программа стандартизации в nanoиндустрии в 2010–2014 гг.», в которой определены приоритетные направления развития стандартизации в nanoиндустрии. К ним относятся:

- разработка национальных стандартов, обеспечивающих широкое применение нанотехнологий в различных отраслях промышленности;
- разработка стандартов, гармонизированных с международными стандартами, обеспечивающих развитие технологической базы, безопасность и конкурентоспособность нанотехнологий и нанопродукции;
- активизация работы участников нанотехнологической сети в работах по стандартизации на национальном уровне;
- целевая подготовка кадров в области стандартизации.

Вышеназванные международные стандарты играют существенную роль в деле развития nanoиндустрии в различных странах. Использование таких стандартов будет способствовать интенсификации процессов, развивающихся в сфере современных технологий, что представляется чрезвычайно важным на современном уровне развития экономики любой страны.

Эти документы обобщают мировой опыт и делают его доступным уже сейчас, пока национальные стандарты большинства стран по нанотехнологиям находятся в стадии разработки. В них, в частности, приводятся рекомендации исследователям и

производственникам по безопасности персонала и потребителя при производстве, хранении, использовании и ликвидации промышленных наноматериалов.

В рамках ЕС, действует множество организационных структур, которые разрабатывают документы и регламенты по различным аспектам использования нанотехнологий, осуществляют менеджмент рисков и контроль исследований в данной сфере.

Так, например, в 2009 г. стартовал проект ЕС под названием Engineered Nanoparticles, Structure, Activity and Toxicology project (ENNSATOX), его цель – исследование влияния наночастиц, широко применяющихся во многих продуктах, на человека и окружающую среду. В рамках проекта повышенное внимание ведущих экспертов из Великобритании, Нидерландов, Бельгии, Италии и Испании уделяется наночастицам оксидов металлов — цинка и титана, которые используются в бытовых моющих, чистящих и дезинфицирующих средствах. Конечная цель проекта — разработать глобальную модель взаимодействия наночастиц с окружающей средой.

С 2005 г. функционирует организованная CRN (Центр ответственных нанотехнологий, США) международная рабочая группа, изучающая социальные последствия развития нанотехнологий. Также тема перспектив развития нанотехнологий как объекта философских исследований обсуждалась на прошедшей в [2007 г.](#) международной футурологической конференции Transvision, организованной [WTA](#) (Всемирная Трансгуманистическая Ассоциация).

Существенная роль в развитии процессов наноиндустриализации отведена и традиционному методу регулирования посредством различного рода межправительственных соглашений, как многосторонних, так и двусторонних. На сегодняшний день подписан ряд международно-правовых договоров, участниками которых является и Российская Федерация, хотя их число еще совсем незначительно, и говорить о первостепенной роли данного метода регулирования в сфере нанотехнологий еще не приходится.

Так, например, в рамках действующего с декабря 2008 г. соглашения о сотрудничестве в сфере нанотехнологий между Финляндией и Россией был проведен круглый стол по стандартизации и регулированию в сфере нанотехнологий. С российской стороны в нем приняли участие представители корпорации РОСНАНО, Всероссийского научно-исследовательского института метрологической службы, Всероссийского научно-исследовательского института стандартизации и сертификации в машиностроении. С финской стороны участвовали специалисты Центра метрологии и аккредитации MIKES, Национального агентства по финансированию технологий и инноваций TEKES, компании Spinverse. Участники обсудили проблемы регулирования в сфере нанотехнологий и подходы к выработке согласованных позиций для представления в европейские агентства по стандартизации и безопасности в контексте реализации потенциальных совместных российско-финских нанотехнологических проектов.

По предложению РОСНАНО сотрудничество по стандартизации и регулированию в сфере нанотехнологий между Россией и Финляндией будет преобразовано в формат рабочей группы.

Подписанный меморандум предусматривает, что взаимодействие Финляндии и России станет основой международного сотрудничества в области регулирования нанотехнологий.

Развитие совместного российско-финского проекта по техническому регулированию и оценке безопасности нанотехнологий и продукции наноиндустрии направлено на создание условий для выхода на мировые рынки конкурентоспособной продукции российско-финских проектов в сфере нанотехнологий.

Дальнейшее сотрудничество будет выгодно для обеих стран, при этом должны учитываться глобальные аспекты. По предложению российской стороны совместные

наработки Финляндии и России в этой сфере могли бы использоваться при интеграции других стран в модель сотрудничества.

Что касается управления развитием NBIC-технологий на международном уровне в рамках уже существующих международных организаций и создания новых регулирующих структур, то данный процесс находится в начальной стадии. Пока можно наблюдать отдельные действия в сфере регулирования биотехнологий и нанотехнологий (см. выше). Хотя в ряде документов отдельно указывается и на особое положение нанобиотехнологий и на перспективы конвергенции биотехнологических методик с информационными и нанотехнологиями.

В документах G8 указывается на необходимость международного сотрудничества в сфере безопасности пищевых продуктов, а также политического диалога, в целях обеспечения устойчивого развития биотехнологии. Отмечается важность работы в данных направлениях таких организаций как комиссия «Codex Alimentarius», Специальная межправительственная целевая группа по пищевым продуктам, полученным при помощи биотехнологии, ОЭСР, ФАО (Продовольственная и сельскохозяйственная организация ООН) и ВОЗ (Всемирная организация здравоохранения). Кроме того, в частности, указывается на прогресс в области медицины, который может последовать в результате расшифровки генома человека и последующих биотехнологических инноваций в соединении с информационными технологиями.

В декларации, принятой по итогам саммита БРИКС (Дели, Индия, 29 марта 2012 г.) утверждается: «Мы отмечаем растущий потенциал НИОКР, а также инноваций в наших странах. Мы поддерживаем процесс сотрудничества как по приоритетным направлениям (продовольствие, фармацевтика, здравоохранение, энергетика), так и в сфере фундаментальных исследований в новых междисциплинарных областях (нанотехнологии, биотехнологии, перспективные материалы и т.д.)».

Особую роль, в данном контексте, играет деятельность ОЭСР.

ОЭСР является авторитетной международной организацией, содействующей обсуждению и поиску эффективных решений проблем социально-экономического развития. Основные направления работы ОЭСР включают кроме прочих и регулирование инновационной сферы (биотехнологии, информационные и коммуникационные технологии, наука и инновации).

ОЭСР располагает 20-летней историей работы в области биотехнологий. В 2005 г. в рамках Международной программы будущего развития ОЭСР стартовал новый проект «Перспективы развития биоэкономики к 2030 г.» (The Bioeconomy in 2030), ориентированный на выработку предварительной программы государственной политики в области биоэкономики.

Утверждается, что последние достижения в биологии, медицине и других науках о человеке претворяют в жизнь прогнозы о скором наступлении эры биотехнологий, о чем уже свидетельствуют серьезные научные разработки в области геномной инженерии, производства модифицированных продуктов питания, экологически чистого биотоплива, продукции микробиологического синтеза, значительно сокращающего энергозатраты, количество потребляемого объема воды и выработку токсичных отходов, получения наносистем и создания материалов на их основе, биоинформатики и во многих других областях. Перспектива развития биотехнологий такова, что уже через 20 лет их использование в повседневной жизни окажется таким же реальным, как и использование современных ИКТ. Ожидается, что применение биотехнологий позволит повысить качество и продолжительность жизни населения как развитых, так и развивающихся стран; улучшить состояние окружающей среды; достигнуть большей эффективности промышленного, сельскохозяйственного и энергодобывающего производства.

Конвергенция биотехнологических методик с информационными и нанотехнологиями способна коренным образом трансформировать процесс производства и структуру потребления товаров и услуг, тем самым открывая новые возможности для

экономического роста, как для развитых, так и для развивающихся стран, и создавая предпосылки для серьезных экономических, социальных и политических изменений.

Проект ориентирован на анализ перспектив биоэкономики в таких областях, как: сельское хозяйство, здравоохранение, промышленность, энергетика, защита окружающей среды и безопасность.

Проект включает построение сценариев возможного развития биоэкономики, основанной на производстве товаров и услуг, учитывающем достижения биотехнологических разработок; определение основных препятствий инновациям в сфере биотехнологий с точки зрения существующих этических, социальных и политических норм, регулирующих инновационную политику наравне с законодательством; проведение количественного анализа возможных преимуществ инновационной политики в указанных областях; а также разработка практических рекомендаций по инновационным решениям в области биотехнологий на международном уровне.

Кроме того, в «Обзоре ОЭСР по науке, технологии и промышленности, 2010» указывается, что современной мировой тенденцией становится развитие таких научных направлений, как: исследования в области биоразнообразия, нейробиологии, геномики человека, регенеративной медицины, прикладного растениеводства. Биотехнологии, нанотехнологии, разработка квантовых компьютеров, изучение сверхпроводимости также являются перспективными направлениями научно-технического развития.

Итак, в настоящее время при рассмотрении процессов регулирования сферы конвергентных технологий в документах международных организаций делается акцент на организацию эффективного сотрудничества государств в данной области. Управление соответствующими технологическими, экономическими, экологическими и социально-политическими рисками обсуждается, в основном, в документах, посвященных проблемам безопасности развития и функционирования либо биотехнологий, либо нанотехнологий по отдельности.

Представляется, что дальнейшее регулирование и контроль всего комплекса NBIC-технологий должны осуществляться как на государственном, так и международном уровнях, причем приоритет должен быть отдан наднациональным институтам. Это объясняется, во-первых, высоким уровнем неопределенности при оценке технологических, экологических, экономических, социально-политических и др. последствий NBIC-конвергенции для цивилизации, что требует упреждающих политических управленческих решений; во-вторых, глобальным характером NBIC-рисков, невозможностью полной локализации отрицательных последствий применения NBIC-технологий; в-третьих, наличием множества неподконтрольных государствам акторов, активно ведущих разработки в указанной сфере, действующих либо из соображений максимизации прибыли либо из др. соображений, не исключая возможностей использования данных разработок в военных, террористических и узкогрупповых целях, несовместимых с безопасным развитием человечества.

Т. о., появление новых рисков, связанных с развитием NBIC-технологий, требует адекватной реакции со стороны всех участников международно-политического процесса. Общий концептуальный подход к управлению рисками в условиях дальнейшего развития NBIC-технологий, заключается в анализе основных факторов воздействия NBIC-технологий на социум; разработке мер, уменьшающих ущерб от воздействия негативных факторов, в том числе до конца неучтенных рисков, непредвиденных обстоятельств; реализации такой системы адаптации населения и общества к рискам, при помощи которой могут быть не только нейтрализованы или компенсированы вероятные негативные последствия, но и максимально использованы шансы для обеспечения высокого уровня безопасности граждан. Эффективное международное сотрудничество – одно из условий решения этих задач.

1.4. Вопросы для самоконтроля

1. Как в сложной системе возникают принципиально новые системные свойства, которые не являются простой суммой свойств элементов системы? Как этот феномен привязать к появлению и возрастанию значимости информационной составляющей глобальной безопасности?
2. Какие технологии являются наиболее критическими по отношению к информационному воздействию?
3. Приведите классификацию информационных войн по М. Либики.
4. Какова роль ТНК в ГИП?
5. Охарактеризуйте ТНК как основных участников информационного противоборства.
6. Проанализируйте действия мирового сообщества по созданию международно-правового режима, регулирующего процессы глобальной информатизации.
7. Каковы особенности рисков NBIC-технологий для человечества?
8. Назовите три основных направления регулирования конвергентных технологий на международном уровне?
9. В чем смысл принципа предосторожности?
10. Охарактеризуйте роль международных организаций в сфере контроля NBIC-процесса.

ГЛАВА 2. Политические коммуникации и проблемы трансформации традиционных СМИ в глобальном интернет-пространстве

2.1. Масс-медийные эффекты глобальной информатизации

К важнейшим факторам жизни современного мирового сообщества можно отнести активно развивающиеся, дополняющие и усиливающие друг друга процессы глобализации и информационной революции, под воздействием которых формируется единое общемировое финансово-информационное пространство. Это, своего рода, высшая стадия интеграции мирохозяйственных связей, информационной, экономической, технологической и культурной взаимозависимости современных государств и народов.

С начала 60-х гг. XX в. соединение воедино и совершенствование средств и каналов передачи информации, создание распределенных компьютерных сетей, электронных баз данных привели на пороге XXI века к возникновению глобального информационного пространства (ГИП) в качестве инфраструктуры современного постиндустриального мира, который все более интегрируется в киберпространство и все более испытывает зависимость от нормального функционирования всех его составляющих. Возникновение ГИП радикально меняет все сферы жизни в планетарном масштабе.

ГИП – это совокупность информационных ресурсов, технологий информационного взаимодействия и информационных телекоммуникационных систем, функционирующих на общих принципах и формирующих информационную инфраструктуру, обеспечивающую информационное взаимодействие между субъектами информационных отношений в масштабах всей планеты.

С одной стороны, ГИП представляет собой результат усилий информационного общества (понимаемого как новая фаза развития цивилизации, в которой главными продуктами производства и обмена выступают информация и знания) стремящегося посредством совершенствующихся информационных технологий максимально удовлетворить свои потребности в коммуникациях, а также в информационных продуктах и услугах в рамках своей политической, экономической и других видах жизнедеятельности. С другой – само информационное общество является порождением ГИП в том смысле, что разветвленная и эффективная информационная инфраструктура способствует развитию общества, повышению ценности информации и коммуникационных процессов, росту влияния информации в целом на общество и на каждого субъекта информационных отношений.

Еще одним актуальным трендом является тот факт, что в настоящее время на мировой арене наряду с государствами активно действуют нетрадиционные акторы (ТНК, СМИ, группы давления, неправительственные организации, внутриполитические регионы, межгосударственные организации, террористические сети и т.п.), которые оказывают растущее влияние на политические тенденции мирового развития. Эти «действующие лица» крайне многочисленны, разнородны, их влияние неоднозначно и, порой трудно «просчитываемо».

Все вышеперечисленные акторы являются также в большей или меньшей степени субъектами ГИП. В современных условиях эффективность их деятельности, организационная структура, а порой и само существование (это касается, например, различных виртуальных сообществ) напрямую зависит от степени «включения» в ГИП, максимального использования всех преимуществ, возможностей и каналов коммуникаций, которые предоставляет им глобальная инфосфера.

Таким образом, мировая политическая система в условиях глобализации и информационной революции имеет тенденцию к усложнению, становится нелинейной, многомерной и многофакторной. А у подобных сложных систем появляются принципиально новые системные свойства или «измерения», с которыми связаны как новые ресурсы глобального развития, так и новые точки уязвимости. Эти свойства проявляются через различные эффекты в различных сферах: военной, экономической, политической, научной, культурной, в сфере безопасности. В частности, в силу вышесказанного, принципиально возрастает роль информационного «измерения» мировой политики и связанной с ним проблематики.

В функционировании СМИ, которые являются главным инструментом политической коммуникации, ярко проявляются эффекты, вызванные глобальным характером информационного пространства. Далее рассмотрены и проанализированы некоторые важные эффекты глобальной информатизации, проявляющиеся в современных масс-медиа.

1. Эффект всеобщей взаимной сопричастности

В современном ГИП любой кризис, любое событие принимает планетарный масштаб, пока на нем сконцентрированы глобальные СМИ. Идея всеобщей и взаимной сопричастности выступает эффективным инструментом манипуляции. С ее помощью проще приучить аудиторию к тому, что события, происходящие в другом полушарии, касаются ее не меньше или даже больше, чем те, что свершаются в собственной стране. Используя включенность человека в ГИП, власти совместно с медиа управляют вниманием граждан, манипулируют повесткой дня, отвлекают человека от одних проблем и, переключая на другие, представляют одни вопросы менее значительными и достойными обсуждения, чем другие – «действительно важные». Таким образом, существует принципиальная возможность выстраивать определенную повестку дня и тем самым влиять на мировое общественное мнение, более того, формировать его и направлять в нужное русло. Мнения аудитории могут разделиться, стороны могут занимать противоположные точки зрения – но лишь в рамках, заданных повесткой дня.

2. Соотношение между глобализацией и демассификацией СМИ

Другой важной особенностью глобальных масс-медиа является следующая дихотомия: с одной стороны, современные технические возможности и взаимосвязанность информационных сетей позволяют оказывать более интенсивное, потенциально неограниченное информационно-политическое влияние на аудиторию, независимо от ее географического положения и гражданской принадлежности; с другой – возрастает необходимость учитывать индивидуальные психологические и культурно-социальные характеристики аудитории. Малые группы и виртуальные сообщества объединяются в информационном пространстве на основе своих узко специальных интересов, сами формируют свои новостные каналы, что не позволяет «охватить» их традиционными СМИ, выводит за рамки влияния традиционными методами.

3. Изменение характеристик политического сообщения в СМИ

В условиях информационной перегрузки важность выбора правильной формы сообщения возрастает: если сообщение не привлечет своего адресата особой манерой подачи и другими выразительными средствами, у его содержания не будет никаких шансов выполнить свою функцию. Форма первична, содержание вторично.

Основными выразительными средствами в коммуникации являются образ и текст. В случае с радио, кино и телевидением к ним добавляется звук – шумовой или музыкальный фон, спецэффекты, интонация речи. Очевидно, что образ обладает наиболее сильным воздействием. 70% всей информации человек получает именно с помощью зрения, в виде образов. Образ первичен по отношению к тексту – он непосредственно отражает реальность и потому понятен без слов, без перевода на иностранные языки. Почти все сообщения в новостных выпусках сегодня – за редким исключением – сопровождаются видеорядом или хотя бы фотографиями. Фото и видео – универсальные

средства коммуникации, которые повествуют о событиях лучше всяких слов. Развитие мультимедийных технологий и средств передачи изображения подняло глобальные коммуникации на новый уровень.

4. Роль СМИ в современных конфликтах

Информационная революция радикальным образом повлияла на ход военного противоборства. Киберпространство наряду с сушей, морем, воздухом и космосом стало новой ареной ведения боевых действий. По сравнению с традиционными войнами значимость информационной составляющей военного конфликта принципиально возросла.

Информационно-психологический аспект военного конфликта становится все более значимым, т.к. в современной ситуации цели войны могут быть успешно достигнуты и невоенными методами, в том числе с использованием всего комплекса СМИ и в глобальном масштабе, и конкретно на театре военных действий. Влияние СМИ на развитие и исход конфликта настолько существенно и неоднозначно, что требует сегодня поиска оптимального баланса между информационной открытостью и эффективностью военной кампании.

Доминирование в информационной сфере является важным фактором победы в современном конфликте. Обретение информационного превосходства рассматривается ведущими державами как эффективное и перспективное средство, позволяющее добиваться внешне- и внутривосточных 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.

Комбинация технологических новаций с методами информационно-психологического воздействия позволила разработать концепцию «операций, ориентированных на результат» (ООР). 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, экономических и политических воздействий. 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.

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.

В настоящее время в обязательном порядке проводится пропагандистская поддержка военных операций в СМИ. Важной частью информационной войны является создание в собственной стране и в глобальном масштабе благоприятного общественного мнения вокруг осуществляемой операции. Например, освещение контртеррористической операции НАТО в Афганистане происходит в рамках четко разработанной пропагандистской кампании. Активность грузинской стороны в СМИ во время грузино-осетинского конфликта 2008 г. так же была в деталях спланирована крупным бельгийским PR-агентством.

Важным аспектом воздействия глобальной информационной инфраструктуры на освещение военного конфликта в СМИ является его прозрачность с информационной точки зрения. В современной ситуации противоборствующие стороны не могут контролировать информацию, т.к. каждый участник конфликта (офицер, рядовой, корреспондент в зоне боевых действий, дипломат, член гуманитарной организации и др.) имеет доступ практически ко всем каналам и средствам связи – мобильной, спутниковой и т.д. Таким образом, масс-медиа в значительной степени стали более независимыми свободными от военной цензуры, что привело к расширению возможностей влияния на общественное мнение.

Характерными особенностями работы СМИ в ходе конфликта являются режим реального времени и эффект CNN.

С одной стороны, новые технические возможности позволяют получить большой объем информации в реальном времени из большого количества стран и регионов, с другой – появляется необходимость переработать это огромное количество (часто противоречивой и без гарантии достоверности) информации и стремительно принимать политические решения. Такая ситуация является серьезной проблемой для дипломатов, политиков военных. Что касается обычных людей, то вал сообщений в реальном времени в быстром темпе, в нескольких фразах с различными комментариями препятствуют ясному пониманию конфликта и его причин, создает дополнительные возможности для манипулирования и дезинформации.

Кроме того, далеко не всегда СМИ занимают независимую объективную позицию при освещении конфликта. Современные технологии позволяют СМИ вмешиваться в ход конфликта в реальном времени. Фильтруя информацию, основываясь на собственной позиции или выполняя чей-либо заказ, поддерживая одну сторону конфликта, СМИ, фактически становятся его участником и несут значительную долю ответственности за его развитие и исход. Сегодня от профессионализма журналиста могут зависеть жизни многих людей и в конечном счете исход конфликтной ситуации. Такое влияние СМИ на конфликтную ситуацию, на позиции противоборствующих сторон и на глобальное общественное мнение называют эффектом CNN.

В киберпространстве с государствами на равных конфликтуют и другие акторы мировой политики (см. выше), причем более слабый участник обладает с одной стороны, преимуществом неуязвимости от информационных атак (по причине слабого развития критической по отношению к информационному нападению инфраструктуры), с другой – возможностью нанести непоправимый ущерб сильному противнику, имеющему разветвленную критическую инфраструктуру.

Концепции «асимметричной» и «сетевой» борьбы предполагают, что основная угроза миру на современном этапе исходит не столько от регулярных армий разных стран, сколько от террористических, криминальных и др. организаций, участники которых объединены в сетевые структуры. Эти транснациональные социальные группы трудно идентифицируются, у них нет постоянного адреса, отсутствует четкая иерархическая подчиненность, у многих из них нет единого руководителя. Они координируют свои действия, используя средства глобальных коммуникаций. Такие структуры имеют единую стратегическую цель, отличаются отсутствием четкого планирования на тактическом уровне и при мобилизации незначительных собственных сил могут вступать в противоборство с бесконечно превосходящим их по силе и возможностям противником.

Современные международные террористические группировки используют ГИП для развития сетевых способов собственной организации, для собственно террористического воздействия на объекты информационной инфраструктуры (кибертерроризм), а получившие широкое распространение новые электронные СМИ становятся организационными и идеологическими узлами указанных террористических сетей, превращаются в инструмент манипуляции массовым сознанием.

Похожим образом действуют и координируют свои усилия по организации «флэш-мобов» движения антиглобалистов, экологические и др. сетевые организации. Через новые СМИ, такие как блоги и социальные сети подобные акции идеологически оформляются и организационно структурируются.

5. «Электронно-цифровой разрыв» и его проявление в СМИ

Важной проблемой, порожденной глобальной информатизацией является «электронно-цифровой разрыв» (digitaldivide), т.е. возникновение элиты, обладающей неограниченным доступом к информации и коммуникационным сетям, как на внутригосударственном, так и на международном уровнях, использующей преимущество владения базами данных и связью в своих узких групповых целях и осуществляющей селективное распределение информации. В результате резко возрастают возможности манипулирования общественным мнением, базирующиеся на разных уровнях доступа отдельных людей, социальных групп, государств и т.д. к информации.

В СМИ на международном уровне цифровой разрыв проявляется при освещении различных событий в развитых странах и странах третьего мира. Например, репортажи о недавней экологической катастрофе в Японии, сопровождались использованием всей возможной технологической мощи современных СМИ и прозвучали соответствующим образом, оказав определенное влияние на мировое общественное мнение – с одной стороны. С другой стороны – недавние этнические волнения в Африке, унесшие почти на порядок больше жизней, чем землетрясение и цунами в Японии, почти не оставили следа в глобальных СМИ и в общественном сознании.

На внутригосударственном уровне цифровой разрыв связан с проблемой доступа к информации, возможностью сравнивать информацию СМИ и критически оценивать ее, что в современных условиях возможно только при определенной степени владения информационными технологиями. Часть населения страны, не владеющая информационными технологиями, оказывается наиболее подвержена влиянию СМИ, манипулирующих информацией в интересах определенных элит или групп.

6. Интеграция СМИ на базе интернет-технологий

Одной из явно прослеживающихся тенденций последнего времени является интеграция СМИ на базе современных цифровых информационно-коммуникационных технологий. В глобальной компьютерной сети появляются и активно функционируют веб-серверы, на которых сконцентрирована, текстовая, аудио-визуальная (интернет-ТВ и радиоканал, например) информация, а так же присутствуют различные интерактивные сервисы, форумы, блоги и даже собственная социальная сеть. Интернет-ресурсы многих традиционных СМИ (телеканалов, радиостанций, газет и журналов) активно развиваются в данном направлении.

Таким образом, процесс политической коммуникации, который во многом реализуется посредством масс-медиа, в условиях глобальной информатизации имеет свои характерные особенности, которые обусловлены новыми системными свойствами современного сложного мира.

Современные СМИ, являясь заметными акторами мировой политики и действуя в рамках глобальной инфосферы, вовлекают в коммуникационные отношения отдельных людей и целые сообщества, государственные и частные организации, экономические, религиозные, культурные институты.

В силу глобального характера информационных отношений СМИ оказывают сегодня большее, чем когда бы то ни было воздействие на формирование сознания и поведение людей, становятся мощным инструментом влияния на институты власти и политический процесс в целом. Понятие СМИ как четвертой власти приобретает новый смысл.

2.2. Интернет-пространство как фактор модернизации институтов гражданского общества

Заявленный руководством страны курс на модернизацию общества требует привлечения значительных ресурсов, в том числе и активизации потенциала граждан, структур гражданского общества. Слабость демократических институтов и структур гражданского общества на современном этапе развития страны является одним из препятствий её модернизации. Как показывает мировая практика реализации модернизационных проектов, одним из условий их успешности является наличие социальных сил, способных стать инициаторами и проводниками перемен.

Гражданское общество в широком смысле представляет собой совокупность общественных институтов, непосредственно не включенных в структуры государства и позволяющих гражданам, их объединениям реализовывать свои интересы и инициативы.

Институты гражданского общества позволяют гражданам вместе выработать цели и достигать их – либо непосредственно совместными усилиями, либо отстаивая в диалоге с другими общественными структурами, бизнесом и носителями власти. Эти институты обеспечивают возможность самореализации, в отличие от институтов, через которые удовлетворяется потребность в доходе. Гражданская активность, в конечном счете, находит выражение в защите и реализации соответствующих прав и свобод человека.

В условиях глобализации и информационного взрыва мир вступил в новую стадию цивилизационного развития. Эффекты новых технологий охватывают все виды человеческой деятельности, информационная технология инициирует сетевую логику изменений социальной системы, информационно-технологическая парадигма основана на гибкости, когда способность к реконфигурации становится «решающей чертой в обществе». Это не могло не отразиться на существенных характеристиках в системе гражданского общества: резко возросла эмансипация личности от государства, сократилось пространство его командного воздействия, произошло энергичное развитие и усложнение горизонтальных социальных связей, сплетение многообразных гражданских институтов и движений в целостную сеть.

Сегодня в условиях современной модернизации в России Интернет-пространство становится инновационной территорией, в рамках которой происходит организация, взаимодействие и структурирование институтов гражданского общества.

1. Эволюция НКО в российском сегменте сети Интернет

В современной ситуации основой гражданского общества являются некоммерческие организации (НКО), которые активно действуют в виртуальном пространстве, используя все возможности интернет-технологий в целях информирования и расширения аудитории своих сторонников, а так же повышения эффективности своей работы.

Некоммерческой, согласно действующему российскому законодательству, считается организация, деятельность которой направлена не на извлечение прибыли, а на решение социально значимых вопросов путем привлечения и целевого использования ресурсов, в том числе благотворительных пожертвований. Российское законодательство предусматривает более 30 различных организационно-правовых форм НКО. На сегодняшний день реальное «действующее ядро» некоммерческого сектора как сегмента гражданского общества России составляет приблизительно 136 тыс. некоммерческих организаций.

Становление некоммерческого сообщества в Интернете можно отнести к началу 1990-х годов. Это связано с периодом наиболее интенсивного его развития в реальности. Начало и середина 1990-х годов для многих НКО являются датой их рождения. В контексте зарождения самостоятельных организаций, независимых СМИ, институтов представительной власти заявить о себе – было важным атрибутом только становящейся

деятельности организаций некоммерческого сектора. Появляются сайты и страницы отдельных организаций. А с середины 1990-х начинает выстраиваться и инфраструктура поддержки НКО по продвижению общественных инициатив в Интернете. Основной мотив действий НКО в сети – презентационный. Трудно подсчитать количество созданных тогда ресурсов, основная часть которых уже прекратила свое существование. Контент этих ресурсов отличался однообразием. Стандартный набор включал: миссию организации, ее историю создания, деятельность и проекты, персоналии и контакты. Такой виртуальный буклет в большей степени был ориентирован на самопрезентацию, чем на взаимодействие с клиентами, партнерами, коллегами и не содержал интерактивных инструментов. Бедность ресурсов была обусловлена и нехваткой профессиональных веб-мастеров, дороговизной и недоступностью их услуг для основной массы НКО. Некоммерческие сайты стали экспериментаторской площадкой для начинающих веб-дизайнеров. В конце 1990-х годов – начале 2000-х Интернет-ресурсы НКО становятся более функциональными и специализированными. Выживают и развиваются самые финансово-устойчивые, ориентированные на сохранение и дальнейшее поддержание созданных виртуальных продуктов. В это время появляются специализированные сайты и сервисные ресурсы, интегрирующие информационную, образовательную, методическую информацию. Начинают формироваться тематические и функциональные Интернет-сообщества: экологических, правозащитных, женских, тренерских, фандрайзерских, донорских и др. организаций, работающих в третьем секторе. Появляется тенденция к регионализации. Интернет становится средством регулярного воспроизведения группового взаимодействия, дешевым способом коммуникации, архивирования информации, отличающимся оперативностью. Разнообразие ресурсов таково: корпоративные сайты (сайты организаций) НКО; сайты проектов, реализуемых в реальной жизни; сайты сервисные (инфраструктурной организации), поисковые каталоги, сайты сетей и сообществ. Идет формирование Интернет-сообщества как группы людей, использующих Интернет в качестве базового средства для организации пространства группового взаимодействия участников. Их деятельность способствует организационному, коммуникационному и образовательному росту сектора в целом. Их роль особенно возрастает, когда речь идет о масштабных проектах российского уровня, затрагивающих интересы сектора в целом (кампания по обсуждению внесения изменений в законодательство об НКО, Налоговый кодекс или Гражданский Форум), когда демонстрация единства сектора по каким-то позициям очень важна.

Важное влияние на сетевую деятельность оказывают такие факторы, как «возраст» НКО, наличие у нее опыта работы, уровень организационного развития, источники финансирования. В целом организации, созданные в постсоветский период, демонстрируют значительную активность в виртуальной сети. Они немногочисленны по своему составу, но в большей степени представлены в Интернете и ориентированы на взаимодействие. Уход части западных благотворительных фондов из поля российского гражданского общества за последние несколько лет вызвал сокращение количества и размеров выдаваемых грантов. Это сказалось и на Интернет-сообществах НКО. Ресурсы стали реже обновляться, часть сайтов оказались брошенными. Увеличение в бюджетах НКО доли российских источников финансирования (гранты ОП РФ, региональные и муниципальные гранты, средства благотворителей) изменяет приоритеты в деятельности НКО. Власти и бизнес ожидают от НКО реальной, а не виртуальной работы с населением.

Сегодня уровень развития общероссийских Интернет-проектов НКО достаточно высок. Это проекты, сумевшие завоевать популярность и имеющие стабильность, ориентированные на внешнюю среду, выполненные на высоком техническом уровне, оформленные в соответствии с современными требованиями к сети, предъявляемыми пользователями. Все больше применяются возможности видео, трехмерной графики, телекоммуникаций в создании виртуальных форумов, конференций, музеев, библиотек, показов видеороликов и т.д.

Интернет-технологии предоставляют большие возможности для объединения НКО в сетевые структуры, тем самым соединяя усилия организаций сектора путем максимально эффективного использования потенциала Всемирной паутины. В отличие от социальных сетей, носящих характер персонального участия («Одноклассники», «В контакте» и др.), сети НКО объединяют организации, не носят такого массового характера и основаны на иных потребностях и ценностях, ориентированных на достижение общественного блага. Практически все ресурсы НКО являются сетевыми. Ссылки, баннеры, разделы «Партнеры» присутствуют на многих сайтах. Сети могут объединять совершенно разные ресурсы (как каталоги и базы данных, так и сайты отдельных НКО). Принципы их создания аналогичны тому, как происходят объединения в реальной коммуникации. Здесь велико значение персоналий, их активности, готовности к взаимодействию. Принципы объединения сетей могут быть: тематическими, региональными, смешанными. Примеры – сети экологических, правозащитных, женских и др. НКО. Сети могут быть разновеликими, объединяя несколько НКО или сотни. Сетевые проекты наиболее интересны там, где в их создании и поддержании участвует не одна организация. Возможности сети позволяют продвигать смежные ресурсы как региональной, так и тематической направленности. Развитие интегрированных ресурсов позволяет включать сети НКО в существующие бизнес-сети, государственные, региональные, гражданские сети, геоинформационные системы и т.д.

На сегодняшний день присутствие некоммерческого сектора в глобальной сети не отражает истинного его разнообразия в реальной жизни. В большей степени «выживают» такие Интернет-продукты НКО, которые ориентированы на клиента, на предоставление востребованной информации, имеют устойчивые и диверсифицированные источники финансирования. Тенденции развития Интернет-деятельности НКО направлены на повышение оперативности информации, укрупнение сетевых объединений, профессионализацию лидеров Интернет-сообщества НКО, переход от форм самопрезентации к более удобному поиску и получению информации и коммуникации в различных формах (виртуальные дискуссии, чаты, форумы, блоги и т.д.). Виртуальное гражданское общество изменяется, развиваясь в русле тенденций реального сектора (от самопрезентации к консолидации и межсекторному взаимодействию). Организации общероссийского масштаба гораздо активнее виртуализируются, демонстрируют более качественные и оперативные ресурсы. Развитие региональных и местных НКО в сети сдерживается финансовыми и техническими возможностями самих организаций и их клиентов. Некоммерческий Интернет-сектор демонстрирует присущие ему в реальной жизни слабости (замкнутость организаций, недостаточную прозрачность, оторванность/слабую связь с населением). Он с осторожностью втягивается в виртуальное пространство, с «оглядкой» на клиентов, с учетом собственных финансовых и технических возможностей и значительно отставая от сетевой деятельности бизнеса и власти.

2. Сетевые сообщества – новые субъекты гражданского общества

На современном этапе, в эпоху глобализации и информационных технологий, гражданское общество не может быть сведено лишь к совокупности организаций. Благодаря сети Интернет, политические процессы и управление приобрели новое содержание, которое обусловило появление новых субъектов гражданского общества – сетевых сообществ. Сетевые сообщества – это относительно неустойчивая совокупность людей, взаимодействующих посредством системы коммуникаций, обеспечиваемых службами сети Интернет, обладающих общностью интересов и осуществляющих совместную деятельность в виртуальном пространстве. Они способствуют формированию « сетевого гражданского общества », цель которого – общение в режиме он-лайн для решения реально существующих социальных проблем.

Главными характеристиками сетевого гражданского общества является «открытость» («установление широких, многомерных связей коммуникации») и

«спонтанность» («свободное формирование, текучесть, постоянное изменение структуры»). Под влиянием сетевых технологий формируется «openspace» – пространство, в котором открываются новые возможности для развития гражданского общества (преодоление отчужденности, неразвитости коммуникаций).

Перевод общественных структур в виртуальное пространство, способствует более продуктивному взаимодействию органов власти и граждан. Здесь важно упомянуть концепцию «цифровой демократии», которая представляет собой сетевое взаимодействие граждан и политических акторов в принятии решений, т.е. сетевая общественность получает возможность влиять на формирование и реализацию публичной политики. Практическое выражение «цифровой демократии» – технология «GOV 2.0» или «правительство 2.0», которая основывается на принципе открытости власти и участия граждан в принятии решений на всех уровнях. Данная технология реализуется через приход чиновников в социальные сети и блогосферу, образование сообществ, где ведется дискуссия с гражданами, имеется доступ к действующим и находящимся в работе законам в режиме он-лайн и другие сетевые практики.

Кроме того, коммуникации в рамках социальных сетей являются наиболее быстрым и действенным инструментом, чем «вертикальная» коммуникация, осуществляемая по государственным каналам; в гражданских сетях производится социальный капитал индивидов, групп и движений как необходимый ресурс гражданского общества, который в будущем будет использоваться для более эффективного взаимодействия в различных ситуациях; указанные сети создают платформу для распространения информации, являются более открытыми, прозрачными и быстрее реагирующими на внешние вызовы, чем другие структуры.

Так же сетевые сообщества наиболее быстро воспринимают инновации в сфере Интернет-технологий. Наряду с уже традиционными технологиями (электронная почта, WWW, мультимедиа, комплекс технологий «SocialSoftware», сетевые платежные системы, он-лайн голосования, мгновенный обмен сообщениями и пр.) это такие как:

- «NETWORK DEMOCRACY» («Сетевая демократия») – технология коллективного принятия решений организаций гражданского общества и правительственных структур на основе прозрачности и открытой повестки дня;
- «SocialBar» – технология позволяющая делиться новостями с друзьями в соцсетях, что дает возможности для структурирования сетевых сообществ и их мобилизации;
- «GlobalVoicesOnline» – международное сообщество добровольцев, которые переводят, суммируют и рассказывают о темах, обсуждаемых по всему миру в блогах, подкастах, видеоблогах и сайтах обмена фотографиями, что позволяет получать свободную и актуальную информацию о событиях в любой точке земного шара.

На базе Интернет-технологий в виртуальном пространстве организационно структурируются и идеологически оформляются новые сетевые сообщества, указанные технологии расширяют возможности взаимодействия всех участников информационных отношений (бизнеса, населения, субъектов гражданского общества, госструктур), способствуют сетевому социальному проектированию, что, в свою очередь, является основой для создания и внедрения инноваций во все сферы жизни общества.

Таким образом, социальные сети (сюда же можно включить блоги, форумы, онлайн-СМИ) становятся важным инструментом формирования гражданского общества, главным фактором его самоорганизации и гражданской мобилизации под влиянием внешних обстоятельств (например, в условиях чрезвычайных ситуаций и природных катастроф), а так же площадками для взаимодействия власти и граждан.

Сильные и влиятельные институты гражданского общества – необходимое условие становления постиндустриального общества, основанного на «экономике знаний». Поэтому стратегические задачи системной модернизации российского общества, перехода к инновационному типу развития выдвинули в центр повестки дня вопрос о расширении

конкуренции, демократии, повышения качества социального капитала и доверия, а также взаимодействия органов власти и гражданского общества. Способность органов власти, бизнеса и гражданских инициатив к партнерству и консолидации в интересах формирования институциональной среды и креативной мотивации, способствующих созданию и внедрению инноваций – одно из важнейших условий инновационного типа развития.

Сегодня Интернет становится инструментом демократии, средой ее обитания. Рождается новый тип прямой демократии – сетевая демократия, которая формирует среду и механизмы мобилизации для проявления активности, для помощи попавшим в беду, для защиты пострадавших и ущемленных, для гражданского активизма и волонтерства, для выстраивания эффективных вертикальных и горизонтальных коммуникаций в обществе, для креативного творчества и аккумуляции социального капитала, для восприятия инноваций. Таким образом, Интернет-пространство является важным фактором, модернизирующим институты гражданского общества в современной России.

2.3. Интернет-коммуникации как средство развития и укрепления русскоязычной диаспоры

В настоящее время Интернет прочно занимает место одного из основных средств коммуникации. Всемирная сеть расширяет коридоры человеческого общения, позволяя людям не только контактировать в информационном пространстве, но и обмениваться опытом, демонстрировать свое творчество, объединяться в группы по интересам, по религиозным взглядам, по идеологическим представлениям. Интернет стирает пространственные границы между людьми, позволяет сохранять и поддерживать общение близких, друзей, родственников, находящихся на разных концах земного шара. В современном мире диаспора становится связующим звеном между Россией и остальным миром, а интернет используется для поддержки и вовлечения диаспоры в экономические, политические и культурные процессы в России. Кроме того, интернет интегрирует соотечественников в информационное поле стран проживания, при этом дает им прекрасную возможность противостоять культурной ассимиляции. В этой связи, хотелось бы уделить особое внимание влиянию Интернета на развитие и укрепление диаспоральных связей.

Одним из общепризнанных признаков диаспоры является пребывание этнической общности людей за пределами страны (территории) их происхождения. Следующий шаг в определении диаспоры состоит в том, что диаспора понимается как такая этническая общность, которая сохраняет важные характеристики национальной самобытности своего народа, содействует развитию национального языка, культуры, сознания. Во времена средневековья число диаспор постоянно возрастало после завоевательных походов войск, в условиях этнических и религиозных преследований, притеснений и ограничений. Новая и новейшая история внесла новую страницу: диаспоры стали появляться в связи с экономическими преобразованиями, потребовавшими значительных трудовых ресурсов (США, Канада, Латинская Америка, Индия, ЮАР, Австралия). Способностью создавать диаспору обладает не каждый этнос, только этнос, устойчивый к ассимиляции. Если объективно устойчивость достигается благодаря фактору организации диаспоры (органы самоуправления, учебные, культурные, политические и др. организации), то субъективно – существованием некоего стержня, будь то национальная идея, историческая память, религиозные воззрения или нечто другое, что сплачивает, сохраняет этническую общность и не позволяет ей раствориться в иноэтнической среде.

Российская диаспора за рубежом считается третьей-четвертой в мире и составляет 30млн человек, причем 20млн проживает в странах СНГ и 10млн — в дальнем зарубежье.

Эти люди отождествляют себя с Россией, ее культурой, не забывают русский язык, тем не менее выбирают местом своего проживания другую страну и интернет в данном случае может стать для российской диаспоры важнейшим средством сохранения и развития родного языка и культурной идентичности.

Во всемирной сети представлены различные сайты, объединяющие соотечественников в данной конкретной стране, например сайт русской диаспоры в Чешской Республике www.ruskadiaspora.cz или www.ruslo.cz. На сайтах освещаются основные культурные, научные, спортивные мероприятия, проходящие под знаком «Русских дней» или «Русских традиций». Безусловно, немисливо существование сайта диаспоры в Интернете без секции форума, где соотечественники могут делиться своими мыслями, проблемами, давать советы туристам. Размещаются адреса и контактные номера телефонов посольств, общественных организаций, занимающихся работой с соотечественниками за рубежом, российские культурные и научные центры. Кроме того, Интернет-ресурс позволяет писателям публиковать свои произведения на родном русском языке. Сайт русскоязычной общины Объединенных Арабских Эмиратов «Русским дом» www.russianhome.com предоставляет информацию, например о магазинах, торгующих русской продукцией, практикующих в Эмиратах русских докторов, позволяет получить юридическую консультацию, ознакомиться с базой данных недвижимости в ОАЭ и прочее.

Такие интернет-проекты как «Русское зарубежье» www.russians.rin.ru позволяют сплотить русские диаспоры по всему миру, кроме того, являются главным источником информации о специфике проживания в той или иной стране для русских, с учетом фактора ментальности. Освещаются проблемы получения гражданства в различных странах, специфика ведения бизнеса за рубежом, проблемы, связанные с образованием и трудоустройством, проблемы приобретения недвижимости и прочее.

Особого внимания заслуживает проблема сохранения и развития родного русского языка вне России, при смене поколений русскоязычной диаспоры. Так, ассоциация «Многоголосое детство» www.enfance-polyphonique.org, созданная группой русскоязычных энтузиастов во Франции занимается вопросами сохранения русского языка у детей, родившихся в двуязычных семьях. Основными трудностями при решении данной задачи являются: давление языковой среды страны проживания; отсутствие русскоязычных школ или их недостаточность; отсутствие мотивации у детей; сложность русского языка по сравнению с западноевропейскими языками. Справочно-информационный интернет-портал ГРАМОТА.РУ, основным направлением деятельности которого является развитие русского языка в сети интернет занимается организацией различных интернет-конференций по вопросам, касающимся в частности воспроизводства русского языка и культуры за пределами России. Так, интернет-конференция под названием «Русский язык вне России: лингвистический и социально-педагогический аспекты взаимодействия культур», предшествовавшая одноименному Международному форуму, состоявшемуся в Берлине в 2005 году, выносила на обсуждения такие темы как: педагогика детского билингвизма: условия и возрастные особенности становления детского двуязычия, приобщения ребенка к двум культурам, условия формирования толерантности; социально-педагогические условия, определяющие выбор оптимальной программы преподавания русского языка в диаспоре: «Русский язык как родной», или «Русский язык как иностранный», или «Русский язык как язык родителей/семьи в иноязычном окружении»; существующие программы, методики, учебные пособия и возможности их педагогического использования в диаспоре, в государственных школах стран Западной Европы и европейских университетах и прочие.

Русская диаспора консолидируется во многом за счет того, что российское государство в последнее время уделяет достаточно много внимания работе с соотечественниками за рубежом. Федеральный закон «О государственной политике РФ в отношении соотечественников за рубежом» 1999 года устанавливает, что

«соотечественниками являются лица, родившиеся в одном государстве, проживающие либо проживавшие в нем и обладающие признаками общности языка, религии, культурного наследия, традиций и обычаев, а также потомки указанных лиц по прямой нисходящей линии». Интернет очень помогает в этом объединении, поскольку является одним из наиболее доступных информационных ресурсов и средств консолидации русского мира.

Существование феномена единения русских соотечественников за рубежом также немислимо без фактора общей национальной идеи, ощущения принадлежности к великому народу с богатыми культурными и духовными традициями. Освоение русской диаспорой всемирной сети Интернет явилось ответом на вызов нового времени стремительно развивающихся информационно-коммуникационных технологий. И в первую очередь, всемирная виртуальная русская сеть направлена на объединение русскоязычных жителей планеты, создание максимально комфортных условий для их общения и самореализации на территории проживания, сохранение традиций и культуры, передачу их из поколения в поколение даже вдали от Родины.

Таким образом, одной из стратегических тенденций, которые обретают значимость в современной ситуации, является быстрорастущий потенциал российской диаспоры. В глобальном мире диаспора становится продолжением гражданского общества, а Интернет предоставляет возможности для полноценного задействования этого потенциала. Кроме того, сетевое сообщество, раздвигая границы государства, резко расширяет юрисдикцию последнего. С появлением стабильных каналов коммуникации появляется и понятие управляемости диаспорой. В частности, это означает также использование ее возможностей для политического лоббизма в значимых для России странах.

2.4. Вопросы для самоконтроля

1. Назовите и охарактеризуйте основные эффекты глобальной информатизации, проявляющиеся в современных масс-медиа.
2. Какова роль СМИ в современных конфликтах?
3. В чем состоит так называемый эффект CNN?
4. Как современное гражданское общество использует интернет-пространство?
5. Охарактеризуйте этапы эволюции российских НКО в интернете.
6. Как сетевые сообщества структурируются в интернет-пространстве и обретают форму реальных организаций?
7. Какие интернет-технологии используют сетевые структуры гражданского общества в своей деятельности?
8. Проанализируйте основные направления деятельности российской диаспоры (в качестве структуры гражданского общества) в Интернет-пространстве.
9. Какие возможности управления диаспорой, а также использования ее для политического лоббизма в значимых для России странах предоставляет Интернет?

ГЛАВА 3. Некоторые особенности современной информационной политики РФ

3.1. Технологии информационного общества как основа российской модернизации

В современной ситуации Россия сталкивается с новыми вызовами модернизации. Основные параметры, по которым российское общество остается не модернизированным были сформулированы Д.А. Медведевым в предвыборных речах и в президентском послании Федеральному собранию: институты – инновации – инфраструктура – инвестиции – интеллект. Это фактически означает признание высшим руководством страны нерешенности ряда задач в социально-экономической области и в сфере государственного строительства.

Если принять тезис, что модернизация – это встраивание в мир, то одним из необходимых условий успешной российской модернизации должно являться формирование внутри страны развитой информационной инфраструктуры и дальнейшая интеграция в глобальное информационное общество.

Проект построения в России информационного общества, сформулированный в ряде официальных документов (в частности в «Стратегии развития информационного общества в Российской Федерации» от 7 февраля 2008 года) в целом лежит в русле перечисленных выше проблем модернизации, так называемых пяти «И».

Поскольку информационная сфера является системообразующей в жизнедеятельности современного государства, постольку она влияет на включенные в нее институты, как государственные, так и институты гражданского общества; экономику; технологическую инфраструктуру; на интеллектуальный потенциал общества.

С одной стороны, в информационном обществе повышается управляемость всеми социально-политическими процессами в стране, с другой – растет эффективность взаимодействия между органами исполнительной и законодательной власти, юридическими лицами и гражданами, возникают дополнительные возможности для функционирования и совершенствования институтов гражданского общества, т.е. в целом развиваются процессы демократизации.

Развитие конкурентоспособной инновационной экономики в стране, транспортной и др. технологической инфраструктуры, повышение доступности медицинских, образовательных и др. услуг так же не возможно без информационной основы. Передовые НИОКР во всех отраслях взаимосвязаны с прогрессом в области информационно-коммуникационных технологий.

И, наконец, в современной ситуации инвестиции в различные проекты в области экономики, социальной сферы, транспорта и т.д. должны предполагать и финансирование информационной составляющей проекта (например, информационных систем управления, геоинформационных систем, систем связи и телекоммуникаций, компьютерных сетей и баз данных), его встроенность в национальное, а в некоторых случаях и в глобальное информационное пространство, без которой данный проект не может быть эффективно реализован.

Таким образом, формирование эффективной государственной информационной политики, направленной на построение в России информационного общества, является необходимым условием и основой успешной модернизации.

Классическая теория рассматривает модернизацию как процесс перехода от традиционного (аграрного) общества к индустриальному, и от индустриального к постиндустриальному. Согласно определению, данному Д. Беллом «постиндустриальное

общество определяется как общество, в экономике которого приоритет перешел от преимущественного производства товаров к производству услуг, проведению исследований, организации системы образования и повышению качества жизни; в котором класс технических специалистов стал основной профессиональной группой и, что самое важное, в котором внедрение нововведений... во все большей степени стало зависеть от достижений теоретического знания». Развитие и внедрение информационно – коммуникационных технологий происходит стремительно быстрыми темпами, в связи с этим все мировое сообщество осознало необходимость и особую важность в формировании эффективной информационной политики. Концепции формирования информационного общества разрабатываются многими государствами на национальном, региональном и международном уровнях. Безусловно, ИКТ развиваются неравномерно, существует проблема «информационной пропасти» между технологически развитыми странами, и странами отсталыми в этом отношении, происходит это преимущественно из-за различий в экономике. Недостаток финансирования этой области, а именно в области ИКТ приводит как так называемой информационной отсталости государства. Данная проблема характерна так же и в пределах одной страны, речь идет об информационном дисбалансе между столицами и периферией.

Впервые необходимость перехода к информационному обществу в России была осознана с разработкой в 1999 году Концепции формирования информационного общества в России по инициативе Государственного комитета Российской Федерации по связи и информатизации и Комитета Государственной Думы по информационной политике и связи. Как следует из концепции «в настоящее время осознаны предпосылки и реальные пути формирования и развития информационного общества в России. Этот процесс имеет глобальный характер, неизбежно вхождение нашей страны в мировое информационное сообщество. Использование материальных и духовных благ информационной цивилизации может обеспечить населению России достойную жизнь, экономическое процветание и необходимые условия для свободного развития личности. Россия должна войти в семью технологически и экономически развитых стран на правах полноценного участника мирового цивилизационного развития с сохранением политической независимости, национальной самобытности и культурных традиций, с развитым гражданским обществом и правовым государством. Годом ранее, а именно 21 декабря 1998 на заседании Постоянной палаты по государственной информационной политике Политического консультативного совета при Президенте Российской Федерации была одобрена Концепция информационной политики Российской Федерации. Областью применения которой, являлась «конкретизация и уточнение основных направлений деятельности органов государственной власти по становлению информационного общества в России, формирование Единого информационного пространства России и ее вхождение в мировое информационное общество». В результате, необходимость построения информационного общества в России стала рассматриваться как «главное условие ее политического и социально-экономического движения вперед и сохранения статуса мировой державы». Признанием того, что развитие информационного общества является важной стратегической компонентой комплексного технологического и инновационного развития страны, стало утверждение в феврале 2008 года Президентом Российской Федерации В.В.Путиным «Стратегии развития информационного общества в России». Одним из основных направлений Стратегии является развитие науки, технологий и техники, а также подготовка квалифицированных кадров в сфере ИКТ – главной движущей силы, способной осуществить переход страны к информационному обществу.

Таким образом, в 2008 году был утвержден ряд нормативных документов, определивших направления развития Российской Федерации на среднесрочную и долгосрочную перспективу, в том числе в части распространения информационных и телекоммуникационных технологий:

Стратегия развития информационного общества в Российской Федерации, утвержденная поручением Президента Российской Федерации от 7 февраля 2008 г. N Пр-212;

Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года, утвержденная распоряжением Правительства Российской Федерации от 17 ноября 2008 г. N 1662-р;

Основные направления деятельности Правительства Российской Федерации на период до 2012 года, утвержденные распоряжением Правительства Российской Федерации от 17 ноября 2008 г. N 1663-р.

Для России главной стратегической задачей становится необходимость изменения содержания экономической и социальной политики государства в направлении перехода на воспроизводственную траекторию развития внутри страны с ориентацией на конечный результат.

Что касается современных государственных инициатив, то Распоряжением Правительства Российской Федерации от 20 октября 2010 года утверждена Государственная программа Российской Федерации «Информационное общество (2011 – 2020 годы)». Цель госпрограммы — создать новые возможности для граждан, бизнеса и государства с использованием ИКТ, а также обеспечить технологический прорыв в использовании информации во всех сферах жизни. В Программе предложен принципиально новый подход к информатизации общества с учётом задач по модернизации экономики. До сегодняшнего дня активность государства в этой сфере была направлена на максимальное использование существующих технологий и возможностей: автоматизацию работы учреждений, налаживание системы межведомственного взаимодействия, интеграцию информационных систем. Сегодня, когда количество информации увеличивается лавинообразными темпами и ее грамотное использование дает огромные возможности, необходимы новые технологии и подходы, которые позволят совершить нашей стране существенный прорыв в области создания и использования высокотехнологичной продукции. Основной принцип формирования программы заключается в том, что её результаты должны приносить пользу конкретным группам потребителей — как гражданам, так и бизнесу. Повышение качества жизни граждан должно выражаться в простых и доступных сервисах, которыми граждане пользуются практически ежедневно: запись на прием ко врачу через Интернет, оплата штрафов с мобильного телефона, недорогой широкополосный доступ во всех общественных местах на территории РФ. Для улучшения условий развития бизнеса основной задачей является обеспечение юридической значимости обмена электронными документами и доступность современной базовой инфраструктуры. Основные направления программы:

- повышение качества жизни граждан и улучшение условий развития бизнеса;
- электронное государство и повышение эффективности государственного управления;
- развитие российского рынка ИКТ и российских технологий, обеспечение перехода к цифровой экономике;
- преодоление цифрового неравенства и создание базовой инфраструктуры информационного общества;
- обеспечение безопасности в информационном обществе;
- развитие цифрового контента и сохранение культурного наследия.

Согласно Концепции государственной информационной политики Российской Федерации 1998 года выделялись три основных класса актуальных проблем построения в России информационного общества. Первый класс составляли проблемы развития технологического базиса информационного общества и перехода к нему. Основными составляющими этого базиса являются: национальные информационные ресурсы и обеспечение свободного доступа к ним; информационно-коммуникационная инфраструктура; научно-производственный потенциал информатизации,

телекоммуникаций и связи; рынок информационных технологий, средств вычислительной техники, телекоммуникаций, связи, информационных продуктов и услуг, и наконец, технологии, структуры и механизмы функционирования и развития электронных СМИ. Ко второму классу проблем относилась проблема обеспечения национальной безопасности, защиты общества и граждан от угроз, связанных с возможностью применения новых информационных технологий в качестве оружия и распространением компьютерных преступлений. Возникла необходимость создания единой системы обеспечения информационной безопасности. Третий класс проблем определялся социально-экономическими и социально-культурными предпосылками перехода России к информационному обществу.

Отрасль информационных и телекоммуникационных технологий в 2000 — 2008 годах развивалась высокими темпами, ежегодный прирост составлял около 25 процентов, что существенно выше среднегодовых темпов роста валового внутреннего продукта и роста отдельных отраслей. Информационные технологии и информационные услуги стали достаточно существенной статьей российского сырьевого экспорта.

Одним из факторов, негативно влияющих на уровень распространения информационных технологий и развитие информационного общества в России на современном этапе, является недостаточно высокий уровень социально-экономического развития многих субъектов Российской Федерации.

По данным Доклада «О развитии информационных и коммуникационных технологий в РФ» общая оценка состояния дел и причин неравномерности развития информационных технологий состоит в следующем: группа регионов, в основном с сырьевой специализацией и развитой промышленностью, имеет необходимые ресурсы для реализации комплексных программ информатизации и успешно использует свое благоприятное экономическое положение. Но значительная доля регионов не в состоянии сегодня осуществлять решение этих задач только за счет собственных средств и значительно отстает в информационно-коммуникационном развитии. Кроме того, на уровень развития информатизации регионов оказывают значительное влияние такие факторы, как понимание руководителями регионов значения и роли информатизации как важнейшего средства повышения эффективности управления и ускорения социально-экономического развития регионов; степень организованности системы управления регионом; наличие квалифицированного кадрового потенциала как в госсекторе, так и в коммерческих ИТ-организациях региона. Отсутствие единой методологии региональной информатизации приводит к низкому качеству планирования и управления реализацией региональных программ и проектов информатизации, неэффективным бюджетным расходам. Программы региональной информатизации слабо увязываются с целями социально-экономического развития региона. Основные направления развития информационных технологий на территориях субъектов Российской Федерации отражены в Концепции региональной информатизации до 2010 года, разработанном Мининформсвязи России с участием заинтересованных федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации. Концепция направлена на реализацию государственной политики в сфере региональной информатизации в соответствии с задачами модернизации государственного управления и социально-экономического развития регионов Российской Федерации. Определена модель финансирования программ региональной информатизации из средств федерального бюджета.

Для ускоренного развития в Российской Федерации информационного общества необходимо обеспечить значительное снижение стоимости предоставляемых населению услуг на основе информационных технологий с одновременным повышением их качества на основе развития конкуренции между операторами связи и поставщиками оборудования.

Следующая проблема, на которой хотелось бы остановиться более подробно, это проблема информатизации образования и дефицита квалифицированных кадров. Информационно - технологические преобразования в сфере дошкольного, среднего и высшего образования приводят к радикальному изменению сущности и организации процессов обучения и развития человека.

Основной стратегической целью развития образования Российской Федерации на среднесрочную перспективу является создание условий для повышения качества человеческого капитала и конкурентоспособности страны. Для достижения этой цели необходимы совершенствование содержания и технологий образования, повышение качества образовательных услуг и эффективности управления в системе образования. При значительном инвестировании средств на разработку цифрового образовательного контента сегодня отсутствуют единые стандарты и требования к его содержанию. Необходимо обеспечить информационную ориентацию образования в целом, включая изменение как методов, так и организационных форм учебного процесса. Требуется разработка и доведение до каждого педагога обновлённых учебных программ, которые позволят подготовить выпускника, способного адекватно ориентироваться в современной информационной среде и самостоятельно выстраивать собственную образовательную траекторию. Определённая часть преподавателей сегодня просто избегает использования современных информационных технологий в своей ежедневной практике. Причина этого – недостаточная подготовка и методологическая поддержка преподавателей по использованию новых возможностей. В результате из высших учебных заведений страны зачастую выходят специалисты, не владеющие современными технологиями и неспособные с их помощью повысить эффективность выполнения функций государственного и муниципального управления.

Следует отметить высокий уровень зависимости российского рынка от зарубежной продукции в сфере информационных технологий. В подавляющем большинстве создаваемых информационных систем в России сегодня используются в основном зарубежные разработки. Можно выделить еще ряд барьеров, препятствующих успешному развитию отечественной промышленности в сфере информационных технологий, среди которых критически значимым является низкий уровень правовой защиты интеллектуальной собственности.

Базис информационной политики, как и политики вообще, составляют совокупность норм права и механизмы их реализации. В данном контексте речь идет о правах граждан, юридических лиц и государства на свободное получение, распространение и использование информации и интеллектуальной собственности. В настоящее время законодательная деятельность по регулированию информационных отношений в российском обществе развивается. Однако действующее законодательство не дает однозначного ответа на ряд принципиальных вопросов, в частности, на какую информацию есть права у граждан, каков состав этих прав, и, наконец, как эти права реализовывать. Поэтому исполнительная и правоприменительная деятельность по реализации указанного законодательства сталкивается с существенными трудностями. Относительно тонкий слой законов в области связи, телекоммуникаций, информации и информатизации позволяет говорить лишь о начале формирования отрасли информационного законодательства в РФ. Действующие федеральные законы «Об информации, информатизации и защите информации», «О связи», а также «О средствах массовой информации» заложили основы законодательного регулирования информационных отношений в обществе с учетом мировой практики, современного уровня развития информационных технологий и обеспечения информационных прав субъектов правоотношений. Можно утверждать, что собственно правовая компонента информационной политики должна предусматривать, прежде всего, формирование правового статуса всех субъектов в системе информационных отношений, пользователей информационных и телекоммуникационных систем (граждане, социальные институты,

общественно-политические организации, органы государственной власти и управления) и определение их ответственности за обеспечение конституционного права на свободу информации.

Информационное общество возникает не только на основе производства и использования компьютеров и сетей передачи данных, но и, главным образом, на базе формирования массовой общественной потребности в информации и ее быстром обращении. Потребность в социальных коммуникациях и стремление населения к получению информации о власти являются следствием зрелости гражданского общества и эффективного функционирования демократических институтов, а не результатом распространения ИКТ. Внедрение ИКТ происходит успешно, если информация активно включается в экономический, политический и культурный оборот, признается ценностью и предметом повышенного потребительского спроса. Именно в связи с этим необходимо формирование информационной культуры в обществе. На сегодняшний день цифровой разрыв коснулся и различных слоев населения, и речь идет здесь не только об информационных возможностях и возможностях доступа к передовым информационным технологиям, существует также проблема ментального характера. Особенно ярко она выражена в разнице восприятия роли ИКТ в жизни общества между разными поколениями людей. Поколение индустриальной эпохи в большинстве своем противится освоению новых информационных технологий в силу традиций, устоев и обычаев, сформировавшихся на протяжении длительного периода жизни данного общества. В связи с этим необходимо проведение специальных мероприятий, направленных на привлечение внимания широких масс к процессу формирования информационного общества в стране. В данном случае, особая роль в этом процессе отводится средствам массовой информации.

Тем не менее, наличие тех или иных проблем на пути становления информационного общества в Российской Федерации не позволяет говорить о невозможности или существенном ограничении в естественном протекании данного процесса. Главным образом, анализ и учет особенностей и специфики современного развития российской информационной и телекоммуникационной инфраструктуры способствует формированию наиболее эффективной государственной информационной политики. В основе «Стратегии развития информационного общества в Российской Федерации» от 7 февраля 2008 года были заложены конкретные цели, задачи, принципы и основные направления государственной политики в области использования и развития ИКТ, науки, образования и культуры для продвижения страны по пути формирования и развития информационного общества. Согласно принятой стратегии «целью формирования и развития информационного общества в РФ является повышение качества жизни граждан, обеспечение конкурентоспособности России, развитие экономической, социально-политической, культурной и духовной сфер жизни общества, совершенствование системы государственного управления на основе использования информационных и телекоммуникационных технологий». В целях реализации принятой стратегии был утвержден план мероприятий, в разработке которого принимают участие федеральные органы исполнительной власти, органы исполнительной власти субъектов РФ, представители бизнеса, научных организаций и гражданского общества. Кроме того, в данном документе имеется приложение, которое носит название «Контрольные значения показателей развития информационного общества в РФ на период до 2015 года». Среди некоторых из этих показателей, которые в ходе реализации Стратегии должны быть достигнуты к 2015 году, хотелось бы отметить следующие: место РФ в международных рейтингах в области развития информационного общества – в числе двадцати ведущих стран мира; место РФ в международных рейтингах по уровню доступности национальной информационной и телекоммуникационной инфраструктуры для субъектов информационной сферы – не ниже десятого; сокращение различий между субъектами РФ по интегральным показателям информационного развития – до 2 раз; доля исследований и

разработок в сфере ИКТ в общем объеме научно-исследовательских и опытно-конструкторских работ, осуществляемых за счет всех источников финансирования: к 2010 году – не менее 15% и к 2015 году – 30%; рост объема инвестиций в использование ИКТ в национальной экономике по сравнению с 2007 годом – не менее чем в 2,5 раза и др.

Таким образом, на современном этапе развития информационного общества в России на государственном уровне предпринимаются серьезные шаги по реализации мероприятий, направленных на формирование эффективной государственной информационной политики. Принятие в 2008 году «Стратегии развития информационного общества в РФ» явилось важным стимулом по реализации программ развития информационной и телекоммуникационной инфраструктуры, а также толчком для решения задач, направленных на преодоление первоочередных проблем на пути становления информационного общества в рамках российского модернизационного проекта. Следующие принятые государственные инициативы отражают нацеленность Правительства Российской Федерации на достижение высоких показателей в сфере развития информационно-коммуникационных технологий.

Главными ориентирами политики развития информационно-коммуникационных технологий в долгосрочной перспективе продолжают оставаться следующие:

1. Формирование современной информационной и телекоммуникационной инфраструктуры.
2. Повышение качества образования, медицинского обслуживания, социальной защиты населения.
3. Обеспечение конкурентоспособности и технологического развития информационно-коммуникационных технологий.
4. Повышение эффективности государственного управления и местного самоуправления, взаимодействия гражданского общества и бизнеса с органами государственной власти.

Всестороннее применение информационных технологий приведет к новому качеству взаимодействия людей в особенности через средства электронных коммуникаций и сеть Интернет, откроет новые возможности для индивидуального развития и развития всех форм хозяйствующих субъектов и органов государственной власти и, как следствие, повысит производительность труда, эффективность и конкурентоспособность экономики.

Приоритетные направления современной модернизации (институты – инновации – инфраструктура – инвестиции – интеллект) предполагают в качестве основы, фундамента создание высокоразвитой информационной инфраструктуры, а так же интенсивное взаимодействие между всеми субъектами информационных отношений как по вертикали, так и по горизонтали, поэтому внедрение технологий информационного общества во все сферы жизнедеятельности государства является необходимым условием успешной российской модернизации.

3.2. Информационная безопасность как важнейший фактор государственной информационной политики Российской Федерации

Термин «Информационное общество» возник в конце 1960-х годов в Японии. Оно стало основным в докладе специальной группы по научным, техническим и экономическим исследованиям, созданной японским правительством для выработки перспектив развития экономики страны. Специалисты определили «информационное общество» как общество, где процесс компьютеризации даст людям доступ к надежным источникам информации, обеспечит высокий уровень автоматизации производства и позволит оптимизировать трудовые процессы.

Информационное общество в трактовке Д. Белла обладает всеми основными характеристиками постиндустриального общества (экономика услуг, определяющая роль теоретического знания, развитие новой интеллектуальной технологии). «В наступающем столетии, - утверждает здесь Д. Белл, - решающее значение для экономической и социальной жизни, для способов производства знания, а также для характера трудовой деятельности человека приобретет становление нового социального уклада, живущего на телекоммуникациях».

А. Тоффлер ввел в научный оборот теорию трех революций, согласно которой человечество пережило уже аграрную и индустриальную революции и стоит на пороге информационной революции.

Американский специалист Ф. Махлуп еще в начале 1960-х годов говорил, что информация может рассматриваться как своего рода промышленный продукт и производство ее — один из видов промышленной индустрии. Об этом же писал чуть позже В.М. Глушков, предложивший концепцию безбумажной технологии в организации сферы управления и распределения в обществе. Но именно японцы стали активными пропагандистами идеи о промышленном значении информации.

Использование информационно-коммуникационных технологий растет в России быстрыми темпами. К примеру, в 2007 году количество ПК в России увеличилось на 35,7% – до 31,2 млн. штук. Также непрерывно растет количество пользователей Интернета – оно уже приблизилось к 35 млн. человек, то есть за год выросло практически на 39,4%. Для устранения информационного неравенства по всей России установлено около 75 тыс. таксофонов и почти 17 тыс. пунктов коллективного доступа к сети Интернет.

Российский рынок продукции и услуг в сфере ИКТ сегодня продолжает развиваться темпами, превышающими среднемировые, – на уровне более 20 процентов в год. Существенную роль в росте количественных показателей сыграли программы внедрения ИКТ в государственное управление, образование и науку. Наиболее важным стал проект по подключению школ к интернету. В рамках этого проекта, который является частью приоритетного национального проекта «Образование», к интернету подключено около 53 тыс. школ в 84 регионах нашей страны.

Признанием того, что развитие информационного общества является важной стратегической компонентой комплексного технологического и инновационного развития страны, стало утверждение в феврале 2008 года Президентом Российской Федерации В.В. Путиным «Стратегии развития информационного общества в России». Одним из основных направлений Стратегии является развитие науки, технологий и техники, а также подготовка квалифицированных кадров в сфере ИКТ – главной движущей силы, способной осуществить переход страны к информационному обществу.

Концептуальную основу формирования информационного общества на среднесрочную и долгосрочную перспективу в России составляют следующие документы: Концепция государственной информационной политики, Концепция формирования информационного общества в России, Доктрина информационной безопасности Российской Федерации, Федеральная целевая программа (ФЦП) Электронная Россия (2002–2010 годы), Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года и др.

Помимо очевидных благ и новых возможностей внедрение ИКТ в жизненно важные сферы жизни общества формирует появление новых вызовов и угроз в сфере сохранности конфиденциальных данных, в области авторского права на публикуемые материалы и т.п. В этой связи политика информационной безопасности должна предопределять информационную политику государства, а не наоборот. Система защиты информации должна работать на опережение и таким образом минимизировать риски утечки информации. Информационная политика государства неразрывно связано с обеспечением информационной безопасности и немислима при ее отсутствии.

Информационные технологии меняют традиционный подход к регулированию отношений между защитой прав на информацию и защитой прав потребителя этой информации. Информационные технологии позволяют из продукта (вещи), каковыми являются компьютер, информационный ресурс или сведение, создать многократно реализуемую услугу, придавая смысл и цель созданию вещи.

С одной стороны, новые информационные технологии позволяют копировать информацию при низких издержках для широкого круга потребителей, с другой – создается конфликтная ситуация, при которой для создателей информации высок риск потери полагающейся им части прибыли.

Проблема несовершенства российского законодательства в сфере информатизации заключается в несогласованности терминологических обоснований в различных законодательных актах в сфере информатизации, а также разногласия в подходах к регулированию как внутри отдельных законов, так и между ними самими.

Ключевой вопрос для информационного законодательства заключается в корректном определении пределов регулирования информационных правоотношений.

Системное развитие нормативно-правового регулирования развития российской информатизации должно осуществляться с учетом регулярной оценки результативности применения существующих нормативных правовых актов в контексте реализации национальной стратегии и вытекающих из нее отраслевых программ социально-экономического развития.

Нормативное правовое обеспечение процессов российской информатизации должно строиться на принципах доступности информации о законодательной деятельности государственных органов, интеграции государственных информационных ресурсов, гармонизации с международным и европейским правом. При развитии нормативной правовой базы речь должна идти не только о разработке и принятии новых законодательных актов, но и об инвентаризации имеющегося нормативного массива, внесении в него изменений.

Среди новых вызовов и угроз информационной безопасности Российской Федерации, помимо отсутствия совершенной нормативно-правовой базы в сфере информатизации, также необходимо отметить недостаточное развитие информационной инфраструктуры, которое наиболее заметно в регионах страны. Таким образом, устранение цифрового разрыва между центром и периферией является одной из приоритетных задач в сфере становления информационного общества. Решением данной проблемы является разработка и реализация региональных программ, направленных на преодоление информационной отсталости между региональным центром и областями.

Отсутствие на российском рынке качественной отечественной электронно-вычислительной, информационно-коммуникационной, аудиовизуальной и пр. продукции также тормозит темп формирования в России полноценной площадки для вхождения в глобальное информационное общество. На российском рынке сегодня преобладают высокотехнологичные новинки западных производителей. Причиной тому является и отсутствие высококвалифицированных специалистов в области ИКТ, и незаинтересованность частных инвесторов во вложении средств в инновационные проекты. Отсутствие интереса обусловлено долгосрочностью проектов и невозможностью быстрого извлечения прибыли.

Система образования России не обеспечивает в необходимом объеме качественное производство трудовых ресурсов, требуемое для повышения конкурентоспособности страны в условиях постиндустриального развития и становления информационного общества, основанного на знаниях. Так, например, потребности страны в специалистах в области ИКТ сегодня удовлетворяются лишь на 40%. Необходима подготовка высококвалифицированных специалистов в сфере ИКТ уже на стадии начальной школы. Внедрение информационных технологий в образовательный процесс позволит сократить цифровое неравенство и в общественной среде.

Основополагающим документом, регулирующим вопросы обеспечения безопасности информационных ресурсов, информационно-телекоммуникационной инфраструктуры и других составляющих национальной безопасности является Доктрина информационной безопасности Российской Федерации. Доктрина представляет собой «совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации» и «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.

Доктрина определяет информационную безопасность России как состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В документе выделяются четыре основные составляющие национальных интересов РФ в информационной сфере:

1. 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.

2. Информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о государственной политике России, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

3. 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, также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

4. Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Согласно анализу состояния информационной безопасности РФ, приведенному в документе, за последние годы в России реализован комплекс мер по совершенствованию ее обеспечения, начато формирование правовой базы, развернута работа по подготовке законопроектов, регламентирующих отношения в информационной сфере. Однако уровень информационной безопасности не в полной мере соответствует потребностям общества и государства.

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.

Доктрина информационной безопасности Российской Федерации прошла длительную и сложную процедуру обсуждения в Межведомственной комиссии Совета

Безопасности Российской Федерации по информационной безопасности, на парламентских слушаниях в Государственной Думе Федерального Собрания Российской Федерации, в средствах массовой информации, на всероссийских и межрегиональных научных конференциях.

Проблема информационной безопасности России является важной частью более общей проблемы обеспечения национальной безопасности страны и существенным образом зависит от стратегии действий государства в этой области.

О необходимости повышения уровня информационной безопасности российского государства отмечается и в Стратегии национальной безопасности Российской Федерации до 2020 года.

Констатируется технологическое отставание в важнейших областях информатизации, телекоммуникаций и связи, определяющих состояние национальной безопасности. Стратегия подтверждает необходимость проведения мероприятий по разработке и внедрению технологии информационной безопасности в системах государственного и военного управления, системах управления экологически опасными производствами и критически важными объектами, а также обеспечения условия для гармонизации национальной информационной инфраструктуры с глобальными информационными сетями и системами.

Кроме того, в документе подчеркивается, что для обеспечения национальной безопасности необходимо сосредоточить усилия на развитие науки, технологий и образования, совершенствование национальных инвестиционных и финансовых институтов в интересах достижения необходимого уровня безопасности в военной, оборонно-промышленной и международной сферах.

Прямое негативное воздействие на обеспечение национальной безопасности в сфере науки, технологий и образования оказывают отставание в переходе в последующий технологический уклад, зависимость от импортных поставок научного оборудования, приборов и электронной компонентной базы, стратегических материалов, несанкционированная передача за рубеж конкурентоспособных отечественных технологий, необоснованные односторонние санкции в отношении научных и образовательных организаций России, недостаточное развитие нормативной правовой базы и слабая мотивация в сфере инновационной и промышленной политики, низкие уровень социальной защищенности инженерно-технического, профессорско-преподавательского и педагогического состава и качество общего среднего образования, профессионального начального, среднего и высшего образования.

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.

Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются:

- создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;
- 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;

○ формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства и пр.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования, а также совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

В последние годы многие эксперты в области внешней политики отмечают, что «многосторонние партнерства» являются эффективным инструментом для решения проблем в сфере информационной безопасности. Сама идея многосторонних партнерств может быть использована для обеспечения инновационного правления, открытого для участия всех заинтересованных сторон.

Россия также участвует в многостороннем партнерстве по формированию структуры международной информационной безопасности в рамках деятельности международных организаций.

Так, например, главы государств Шанхайской Организации Сотрудничества (ШОС), в состав которой входят Китай, России, Казахстан, Таджикистан, Киргизия и Узбекистан поддерживают деятельность, осуществляемую в рамках Организации Объединенных Наций по рассмотрению существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, а также исследованию соответствующих международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем, и полагают важным продолжать ее.

Наряду с этим, главы государств выражают озабоченность тем, что в настоящее время появляется реальная опасность использования ИКТ в целях, способных нанести серьезный ущерб безопасности человека, общества и государства в нарушение основополагающих принципов равноправия и взаимного уважения, невмешательства во внутренние дела суверенных государств, мирного урегулирования конфликтов, неприменения силы, соблюдения прав человека.

Главы государств подчеркивают, что трансграничный характер ИКТ, современных вызовов и угроз диктует необходимость дополнения национальных усилий по обеспечению информационной безопасности совместными действиями на двустороннем, региональном и международном уровнях.

Главы государств заявляют о близости позиций своих стран по ключевым проблемам, связанным с международной информационной безопасностью (МИБ), и намерены объединить усилия в рамках ШОС в целях противостояния новым информационным вызовам и угрозам с соблюдением принципов и норм международного права, включая Устав ООН и Всеобщую декларацию прав человека. В этой связи главы государств приняли решение о создании группы экспертов государств - членов ШОС по МИБ с участием представителей Секретариата Организации и Исполкома Региональной антитеррористической структуры для выработки плана действий по обеспечению международной информационной безопасности и определению возможных путей и средств решения в рамках ШОС проблемы МИБ во всех ее аспектах.

Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО), в работе которой на всех этапах активно участвовала и Россия, провозгласила доверие и безопасность главными опорами информационного общества. В ходе Женевского этапа (10-12 декабря 2003 года) был разработан План действий, в соответствии с которым участники Встречи определили конкретные направления деятельности, которые ведут к достижению согласованных на международном уровне целей развития информационного общества. Одним из направлений действий является

укрепления и доверия и безопасности при использовании ИКТ и включает в себя следующие задачи:

1. Содействовать сотрудничеству между государствами в рамках Организации Объединенных Наций и со всеми заинтересованными сторонами в рамках соответствующих форумов с целью укрепления доверия пользователей, повышения надежности и защиты целостности как данных, так и сетей; анализа существующих и потенциальных угроз в области ИКТ; а также решения других вопросов информационной безопасности и безопасности сетей.

2. Органам государственного управления в сотрудничестве с частным сектором необходимо предупреждать, обнаруживать проявления киберпреступности и ненадлежащего использования ИКТ и реагировать на эти проявления путем разработки руководящих принципов, которые учитывали бы ведущуюся в этой области работу; изучения законодательства, которое дает возможность эффективно расследовать и подвергать преследованию ненадлежащее использование; содействия эффективным мерам взаимопомощи; усиления на международном уровне институциональной поддержки профилактики таких инцидентов, их обнаружения и ликвидации их последствий; а также путем содействия образованию и повышению осведомленности.

3. Органы государственного управления и другие заинтересованные стороны должны активно поощрять обучение пользователей и повышать их осведомленность относительно неприкосновенности частной жизни при работе в онлайн-режиме и способов ее защиты.

4. Принимать необходимые меры на национальном и международном уровнях для защиты от спама.

5. Поощрять проведение на национальном уровне оценки внутреннего законодательства с целью ликвидации препятствий для эффективного использования документов и осуществления сделок в электронной форме, в том числе использования электронных методов аутентификации.

6. Продолжать укрепление надежности и безопасности с помощью взаимодополняющих и взаимоусиливающих инициатив в сфере безопасности при использовании ИКТ и инициатив или руководящих принципов в отношении прав на неприкосновенность частной жизни, защиту данных и прав потребителей.

7. Обмениваться образцами наилучшей практики в области информационной безопасности и безопасности сетей и поощрять их использование всеми заинтересованными сторонами.

8. Предложить заинтересованным странам назначить координаторов для реагирования в режиме реального времени на происшествия в сфере безопасности и объединить этих координаторов в открытую совместную сеть для обмена информацией и технологиями реагирования на происшествия.

9. Поощрять дальнейшее развитие безопасных и надежных приложений для упрощения осуществления сделок в онлайн-режиме.

10. Поощрять активное участие заинтересованных стран в проводимой Организацией Объединенных Наций деятельности по укреплению доверия и надежности при использовании ИКТ.

Таким образом, в современных условиях информационная безопасность становится важнейшим базовым элементом всей системы национальной безопасности российского государства. Обусловлено это, прежде всего, быстро растущими технологическими возможностями современных информационных систем, которые по своему влиянию на политику, хозяйственно-экономическую жизнь, духовно-идеологическую сферу и умонастроения людей стали в настоящее время решающими и всеохватывающими.

Кроме того глобальная информатизация общества чрезвычайно обострила проблему обеспечения информационной безопасности государства, что определяет

необходимость разработки и постоянного совершенствования соответствующей государственной политики в этой сфере.

3.3. Вопросы для самоконтроля

1. Каким образом успех современной российской модернизации (по параметрам пять «И») зависит от формирования внутри страны развитой информационной инфраструктуры и дальнейшей интеграции в глобальное информационное общество?
2. Охарактеризуйте основные направления информационной политики Российской Федерации и государственные инициативы по становлению информационного общества (в плане внедрения информационно-коммуникационных технологий в важнейшие сферы жизнедеятельности государства).
3. Назовите приоритетные направления информационной политики РФ в контексте обеспечения информационной безопасности государства.
4. Проанализируйте содержание базовых документов РФ в сфере обеспечения информационной безопасности.
5. Охарактеризуйте деятельность России в рамках международных организаций в области информационной безопасности и нормативно-правового регулирования развития информационно-коммуникационных технологий.

ЗАКЛЮЧЕНИЕ

Таким образом, новейшие информационные технологии становятся одним из наиболее важных факторов управления современным миром, основным инструментом власти, влияющим на сложившуюся систему международных отношений и трансформирующим саму концепцию как национальной, так и международной безопасности.

Мировая политическая система в информационную эпоху характеризуется следующими основными тенденциями:

- глобализация как процесс формирования единого общемирового финансово-информационного пространства;
- информационная революция (качественно новый этап развития и внедрения информационных технологий) и ее влияние на современный мировой политический процесс (МПП), в частности, на три составляющие МПП (субъекты МПП – мировое сообщество; содержательная сторона МПП, т.е. международные отношения; безопасность).

Международно-значимыми результатами трансграничного информационного обмена являются:

- децентрализация, прозрачность границ, плюрализм;
- появление новых негосударственных акторов (структур и субъектов глобального информационного пространства), действующих в международном масштабе, сетевая организация сообществ;
- эрозия государственного суверенитета в условиях глобализации и информационной революции: адаптация государства к новым условиям;
- новая экономика информационной эпохи – снижение возможностей государственного управления и контроля в экономической сфере;
- 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 национальной и международной безопасности, изменение форм международных конфликтов (информационная война), компьютерная преступность, компьютерный терроризм;
- формирование глобального трансграничного информационного пространства, интернет как глобальная информационная среда, как важнейшая составляющая инфраструктуры постиндустриального (информационного) общества.
- новое качество политических коммуникаций: электронное правительство, электронная демократия, формирование и структурирование гражданского общества на базе сетевых интернет-сообществ (как на национальном, так и на международном уровнях).

Можно утверждать, что система международно-правового регулирования технологического развития будет формироваться по двум взаимосвязанным направлениям:

- первое состоит в максимальном расширении позитивных возможностей, которые предоставляют новейшие технологии мировому сообществу,
- а второе — в минимизации рисков и негативных последствий, которые влечет для человечества развитие комплекса указанных технологий.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

а) основная литература:

1. Глобализация. Контуры целостного мира [Электронный ресурс] / Чумаков А.Н. - М. : Проспект, 2017. - <http://www.studentlibrary.ru/book/ISBN9785392215621.html>
2. Государственная информационная политика в условиях информационно-психологической войны [Электронный ресурс] / Манойло А.В., Петренко А.И., Фролов Д.Б. - 3-е изд., стереотип. - М. : Горячая линия - Телеком, 2012. - <http://www.studentlibrary.ru/book/ISBN9785991202534.html>
3. Западная социология: современные парадигмы : антология [Электронный ресурс] / сост., авт. библиогр. очерков Г.Н. Соколова, Л.Г. Титаренко - Минск : Белорус.наука, 2015. - <http://www.studentlibrary.ru/book/ISBN9789850818140.html>
4. Интеллект и технологии: монография [Электронный ресурс] / Алексеева И.Ю., Никитина Е.А. - М. : Проспект, 2016. - <http://www.studentlibrary.ru/book/ISBN9785392204632.html>
5. Интернет вещей: Будущее уже здесь [Электронный ресурс] / Грингард С. - М. : Альпина Паблишер, 2016. - <http://www.studentlibrary.ru/book/ISBN9785961458534.html>
6. Интернет-аналитика. Поиск и оценка информации в web-ресурсах. Практическое пособие. - М.: Книжный мир, 2012. - 78 стр. - <http://www.studentlibrary.ru/book/ISBN9785804105694.html>
7. Интернет-СМИ: Теория и практика [Электронный ресурс] : Учеб. пособие для студентов вузов / Под ред. М.М. Лукиной. - М. : Аспект Пресс, 2013. - <http://www.studentlibrary.ru/book/ISBN9785756705423.html>
8. Информационная безопасность и вопросы профилактики кибер-экстремизма среди молодежи [Электронный ресурс] / Чусавитина Г.Н. - М. : ФЛИНТА, 2014. - <http://www.studentlibrary.ru/book/ISBN9785976520387.html>
9. Информационное право. Конспект лекций: учебное пособие [Электронный ресурс] / Михельсон К.К. - М. : Проспект, 2016. - <http://www.studentlibrary.ru/book/ISBN9785392195244.html>
10. Информационные правоотношения: теоретические аспекты [Электронный ресурс] / Морозов А.В. - М. : Проспект, 2017. - <http://www.studentlibrary.ru/book/ISBN9785392240920.html>
11. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов - М. : ДМК Пресс, 2018. - <http://www.studentlibrary.ru/book/ISBN9785937000323.html>
12. Коммуникология: теория и практика массовой информации [Электронный ресурс] / Шарков Ф.И. - М. : Дашков и К, 2017. - <http://www.studentlibrary.ru/book/ISBN9785394026713.html>
13. Личность и общество: информационно-психологическая безопасность и психологическая защита [Электронный ресурс] / Г.В. Грачев. - М. : ПЕР СЭ, 2003. - <http://www.studentlibrary.ru/book/ISBN5929201013.html>
14. Международное управление Интернетом: конфликт и сотрудничество [Электронный ресурс]: учеб.пособ. / Е.С. Зиновьева - М. : МГИМО, 2011. - <http://www.studentlibrary.ru/book/ISBN9785922807012.html>
15. Модели диалога власти и общества в интернет-коммуникациях [Электронный ресурс] / под общ.ред. Л.А. Василенко, Е.В. Тарасовой - М. : Проспект, . - <http://www.studentlibrary.ru/book/ISBN9785392180905.html>

16. Новая информационная экономика и сетевые механизмы ее развития [Электронный ресурс] / Лазарев И. А. - М. : Дашков и К, 2013. - <http://www.studentlibrary.ru/book/ISBN9785394006265.html>
17. Новые информационные коммуникационные технологии в образовании [Электронный ресурс] / Трайнев В. А. - М. : Дашков и К, 2013. - <http://www.studentlibrary.ru/book/ISBN9785394016851.html>
18. Приемы информационных войн: Учеб.пособие для студентов вузов [Электронный ресурс] / Вирен Г. - М. : Аспект Пресс, 2017. - <http://www.studentlibrary.ru/book/ISBN9785756708240.html>
19. Современное общество: общество риска, информационное общество, общество знаний [Электронный ресурс] / ГоттхардБехманн - М. : Логос, 2017. - <http://www.studentlibrary.ru/book/ISBN9785987044568.html>
20. Социология информационного общества [Электронный ресурс]: учебное пособие / Игнатъев В.И. - Новосибирск : Изд-во НГТУ, 2016. - <http://www.studentlibrary.ru/book/ISBN9785778229433.html>
21. Футурология. XXI век: бессмертие или глобальная катастрофа? [Электронный ресурс] / Турчин А.В. - М. : БИНОМ, 2013. - <http://www.studentlibrary.ru/book/ISBN9785996315215.html>
22. Что такое общество знаний? [Электронный ресурс] / Алексеева И.Ю. - М. :Когито-Центр, 2009. - <http://www.studentlibrary.ru/book/ISBN9785893533163.html>
23. Экономика России и Европы в эпоху глобализации. Экономическое развитие, механизмы управления и информатизации стран европейского союза [Электронный ресурс] / Агузаров З.А., Агузарова Л.А., Алешин А.В. - Ростов н/Д : Изд-во ЮФУ, 2012. - <http://www.studentlibrary.ru/book/ISBN9785927510122.html>

б) дополнительная литература:

24. Абдеев Р.Ф. Философия информационной цивилизации. - М., 1994.
25. Анохин М.Г., Комаровский В.С. Политика: возможность современных технологий. - М.,1998.
26. Анохин М.Г., Павлютенкова М.Ю. Информационно-коммуникативные технологии в политике. // Вестник Российского университета дружбы народов. – Сер.: Политология. – 1999. – № 1.
27. 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.
28. Багиров А. Новые информационные технологии в международных отношениях. // Международная жизнь, 2001, №8.
29. Балугев Д.Г. Завоевание будущего: внешняя политика России на рубеже веков: Монография. - Н.Новгород: ИСИ ННГУ,1999. - 122 с.
30. Балугев Д.Г. Информационная революция и современные международные отношения: Уч. пособие. - Н.Новгород: ННГУ, 2001. - 107 с.
31. Балугев Д.Г. Новые информационные технологии и современные международные отношения. - Н.Новгород: ННГУ, 1998. - 47 с.
32. Белл Д. Грядущее постиндустриальное общество. - М.: Academia, 1999.
33. 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.
34. В.Л. Иноземцев. Современное постиндустриальное общество. - М.: Логос, 2000.
35. Василенко В.И., Василенко Л.А. Интернет в системе государственной службы. - М., 1998.

36. Васильев Г.Г. Становление информационной цивилизации и тенденции обновления регулятивной системы общества. // Роль государства в формировании современного общества. - М., 1998.
37. Воронина Т.П. Информационное общество: сущность, черты, проблемы. - М., 1995.
38. Григорьев М.С. Политические коммуникации в «век информации». // Политическое управление: Сборник научных трудов кафедры политологии и политического управления. - М., 1998.
39. Гудков В.В. Государство и информационное общество. // Труды Московской государственной юридической академии. - 1999. - № 4.
40. Дайсон Э. Жизнь в эпоху Интернета. Release 2.0. - М.: Бизнес и Компьютер, 1998. - 400 с.
41. Даниелов А.Р. Россия в мировой системе высоких технологий: формирование информационного общества. // США: Экономика, политика, идеология. - 1996. - № 9.
42. Дмитриев А.В., Латынов В.В., Хлопьев А.Т. Неформальная политическая коммуникация.—М., 1996.
43. Доброхотов Р.А. Политика в информационном обществе. // Полис, 2004, №3.
44. Егоров В.С. Человек информационный. // Человек, наука, управление. - М., 2000.
45. Егоров Э.Н. Информационное общество. М., 1993.
46. Запад: новые измерения национальной и международной безопасности: Монография. - Н.Новгород: ННГУ, 1997. - 348 с.
47. Иларионова Т.С. Информационные процессы в современной России. - М., 1999.
48. Иноземцев В.Л. Современное индустриальное общество: природа, противоречия, перспективы. - М., 2000.
49. 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.
50. Информационное обеспечение государственного управления. / Авт.: Никитов В.А., Орлов Е.И., Старовойтов А.В., Савин Г.И.; Под ред. Ю.В.Гуляева. - М., 2000.
51. 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.
52. Кастельс М. Информационная эпоха: Экономика, общество и культура. М., 2000.
53. Кашлев Ю. Международные отношения в зеркале информационной революции. // Международная жизнь, 2003, №1.
54. Кедровский О.В. Информационная среда обитания. // Информационные ресурсы России. - 1995. - № 3.
55. Кеннеди П. Вступая в двадцать первый век. - М.: Весь Мир, 1997. - 480 с.
56. Клепцов М.Я. Информационные системы органов государственного управления. - М., 1996.
57. Колин К.К. Наука для будущего: социальная информатика. // Информационные ресурсы России. - 1995. - № 3.
58. Компьютеризация общества и человеческий фактор. Реферативный сборник/ Отв. Ред. А.И. Ракитов. - М.: ИНИОН АН СССР, 1988. - 228 с.
59. Кристиансон М. Подход к анализу информационной политики, основанный на изменениях в глобальных экономических силах // Международный форум по информации и документации. - 1996. - т.21. - №1.
60. Лагутина М.Л. Объективные условия формирования глобальной системы. // Россия в глобальном мире. Ч.1. СПб., 2004.
61. Лагутина М.Л. Роль глобализации в формировании новой системы международных отношений. // Россия в глобальном мире. СПб., 2006.
62. Лисичкин В.А., Шелепин А.А. Третья мировая (информационно-психологическая) война. - М.: Институт социально-политических исследований АСН, 2000. - 304 с.

63. 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.
64. Мелюхин И.С. Информационное общество: истоки, проблемы, тенденции развития. - М., 1999.
65. Мешкова Т.А. Социально-политические аспекты глобальной информатизации // Полис. - 2002. - № 6.
66. Модестов С.А. Информационное противоборство как фактор геополитической конкуренции. (Серия «Научные доклады», вып. 74.) - М.: МОНФ; Издательский центр научных и учебных программ, 1999. - 64с.
67. Моисеев Н. Информационное общество как этап новейшей истории. // Свободная мысль, 1996, №1.
68. Мур Н. Права и обязанности в информационном обществе. // Научные и технические библиотеки. - 1999. - № 1.
69. Мухин А.А. Информационная война в России.—М., 2000.
70. Нисневич Ю.А. Информационная политика России: проблемы и перспективы. - М., 1999.
71. Нисневич Ю.А. Информация и власть. - М., 2000.
72. Новая постиндустриальная волна на Западе. Антология/ Под ред. В.Л. Иноземцева. - М.: Academia, 1999.
73. Панарин И.Н. Информационная война и Россия.—М.. 2000.
74. Пасхин Е.Н. Информатизация образования в стратегии устойчивого развития: философско-методологический анализ. - М., 1999.
75. Перфильев Ю.Ю. Российское Интернет-пространство: развитие и структура. М., 2003.
76. Попов В.Д. Информациология и информационная политика. - М., 2001.
77. Поппель Г., Голдстайн Г. Информационная технология - миллионные прибыли. - М.: Экономика, 1990. - 238 с.
78. Постиндустриальный мир: Центр, Периферия, Россия. Общие проблемы постиндустриальной эпохи. (Серия «Научные доклады», вып. 91.) - М.: МОНФ; ИМЭМО РАН, 1999. - 304с.
79. Постиндустриальный мир: Центр, Периферия, Россия. Особый случай России. (Серия «Научные доклады», вып. 93.) - М.: МОНФ; ИМЭМО РАН, 1999. - 224с.
80. Почепцов Г.Г. Информационно-психологическая война. - М.: СИНТЕГ, 2000. - 180 с.
81. Почепцов Г.Г. Коммуникативные технологии XX века. - М., 1999.
82. Прайс, Монро. Телевидение, телекоммуникации и переходный период: право, общество и национальная идентичность.- М., 2000.
83. Проблема трансграничности информации. Интеграция пространства и сетевая несвобода. // МЭМО, 2000, №11.
84. Пугачев В.П. Средства массовой коммуникации в современном политическом процессе // Вестник МГУ. - Серия 12: Политические науки. - 1995. - № 5.
85. Ракитов А.И. Информация, наука, технология в глобальных исторических изменениях. - М.,1998.
86. Ракитов А.И. Философия компьютерной революции. - М., 1991.
87. Расторгуев С.П. Философия информационной войны. - М.: Вузовская книга, 2001. - 468 с.
88. Римский клуб/ Сост. Д.А. Гвишиани, А.И. Колчин, Е.В. Нетесова, А.А. Сейтов. - М.: УРСС, 1997. - 384 с.
89. Сидоров В.А. Политическая культура средств массовой информации. - М., 1994.
90. 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.

91. Слипченко В.И. Война будущего. (Серия «Научные доклады», вып. 88.) - М.: МОНФ; Издательский центр научных и учебных программ, 1999. - 292с.
92. 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.
93. Стоуньер Т. Информационное богатство: профиль постиндустриальной экономики // Новая технократическая волна на Западе. - М., 1986.
94. Технологии в политике и политическом управлении. / Под ред. Анохина М.Г., Комаровского В.С., Матвеевко Ю.И. - М., 2000.
95. Тоффлер А. Третья волна. - М.: АСТ, 1999. - 748 с.
96. Уэбстер Ф. Теории информационного общества. М., 2004.
97. Хакен Г. Информация и самоорганизация. - М.: Мир, 1991.
98. Шретмен К.А. Управление информацией в 90-е годы: концептуальные основы. // Международный форум по информации и документации. - 1993. - № 2. - Т. 18.
99. Юзвишин И.И. Основы информациологии. - М., 2000.
100. Addington, Larry H. The patterns of war since the eighteenth century. - Bloomington and Indianapolis: Indiana University Press, 1994. - 362 p.
101. Alberts, David S. Defensive information warfare. - Washington DC: NDU Press, 1996. - 82 p.
102. De Landa, Manuel. War in the age of intelligent machines. - New York: Swerve Editions, 1991. - 272 p.
103. Libicki, Martin C. Defending cyberspace and other metaphors. - Washington DC: NDU Press, 1997. - 110 p.
104. Libicki, Martin C. What is information warfare? - Washington DC: NDU Press, 1995. - 104 p.
105. Shukman, David. Tomorrow's war: the threat of high-technology weapons. - New York/San Diego/London: HarcourtBrace&Company, 1996. - 272 p.
106. Van Creveld, Martin. Technology and war: from 2000 B.C. to the present. - New York: The Free Press. 1991. - 342 p.
107. 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.

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. Бжезинского - 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. Бжезинского, 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. Бжезинского, 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 МануэляКастельса.
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 (FreedomofexpressionandsecurityontheInternet) 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. Интернационализованные 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 -2018.
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. «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. Стратегические вопросы.
8. ИКТ в национальных проектах. ИТ в здравоохранении – международный опыт и развитие здравоохранения в России.
9. ИКТ в национальных проектах. ИКТ в образовании – международный опыт и развитие в России.
10. ИКТ в национальных проектах. ИТ в ЖКХ – опыт и возможности.
11. ИКТ в национальных проектах. ИТ в АПК – опыт и возможности.
12. Развитие ИКТ, «новой экономики» и высокотехнологичных отраслей как условия стратегического развития России в политической повестке дня.

Алексей Евгеньевич **Белянцев**
Вадим Анатольевич **Берендеев**
Игорь Валерьевич **Шамин**

НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МИРОВОЙ ПОЛИТИКЕ

Учебно-методическое пособие

Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет им.
Н.И. Лобачевского».
603950, Нижний Новгород, пр. Гагарина, 23