САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

На правах рукописи

КУЧЕРЯВЫЙ Михаил Михайлович

ИНФОРМАЦИОННОЕ ИЗМЕРЕНИЕ ПОЛИТИКИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ В УСЛОВИЯХ СОВРЕМЕННОГО ГЛОБАЛЬНОГО МИРА

Специальность:
23.00.04 – политические проблемы международных отношений, глобального и регионального развития

Диссертация на соискание ученой степени доктора политических наук по специальности

Научный консультант: Косов Юрий Васильевич,
доктор философских наук, профессор

Санкт-Петербург
2014

Оглавление

ВВЕДЕНИЕ

Актуальность темы исследования. В современном мире нарастают противоречия геополитического и геоэкономического характера, усиливается конкуренция между отельными ведущими государствами, группами государств и макрорегионами. Эти процессы протекают на фоне вступления человечества в новую фазу развития, связанную со становлением глобального информационного общества. В данных условиях проблемы обеспечения национальной безопасности приобретают для Российской Федерации жизненно важный характер. В связи с этим возникает настоятельная необходимость модернизации всей системы национальной безопасности нашей страны. Во-первых, во время структурного кризиса 1990-х годов, следствием которого стало резкое ограничение ресурсов и возможностей, сфера обеспечения национальной безопасности России не получила должного развития. Компенсация этого отставания осуществляется в наши дни. Очевидно, что модернизационный подход позволяет решить эту задачу на качественно ином уровне, чем это было возможно два десятка лет тому назад.

Во-вторых, существенное изменение геополитической картины современного мира, связанное с усилением тенденции перехода к многополярному миру и агрессивным устремлением США и их союзников сохранить мировой порядок, сложившийся в период монополярной системы международных отношений, значительно увеличивает риски в обеспечении национальной безопасности Российской Федерации и международной безопасности в целом.

В-третьих, стремительное развитие информационно- коммуникационных технологий, создание глобального информационного пространства коренным образом усилили значение информационной составляющей в обеспечении национальной и международной безопасности. Мировое информационное пространство тесно связано с другими сегментами международного сообщества – экономическим, политическим, военным, социальным и другими сферами

жизнедеятельности. Все большее влияние на обеспечение национальной и глобальной безопасности оказывают в мировом сообществе следующие факторы: глобализация современного мира и происходящие в нем политические процессы, информатизация всех основных сфер жизнедеятельности мирового сообщества и индустриально развитых стран, переход от индустриальной стадии развития общества к постиндустриальным информационным, политическим, экономическим, военным и социальным системам. Инновационное развитие сил и средств обеспечения информационной составляющей национальной безопасности должно стать магистральным направлением модернизации всей системы национальной безопасности.

Обеспечение национальной безопасности нашей страны от угроз представляет собой важную задачу как в теоретическом, так и в практическом аспектах. Актуальность и сложность этой задачи возрастает при рассмотрении ее применительно к информационному пространству в новых геополитических условиях второго десятилетия XXI века.

Это обусловлено целым рядом обстоятельств. Прежде всего тем, что информационное пространство становится все больше связано с мировыми геополитическими процессами. Вопросы формирования и развития глобального информационного общества находятся в фокусе мировой политики. Далее, прогресс в развитии информационно-коммуникационных технологий открывает принципиально новые возможности как для устойчивого роста экономики, так и для укрепления обороноспособности современных развитых государств. Следовательно, развитие информационной сферы представляет собой важное направление политики модернизации российского государства.

В то же время постоянное расширение возможностей информационно-коммуникационных технологий, все большая зависимость от их успешного применения во всех основных сферах общественной жизни постоянно повышает уязвимость современного государства от угроз его национальной безопасности, которые возникают в глобальном информационном пространстве.

В современных условиях информационная безопасность рассматривается как важная составляющая системы обеспечения национальной безопасности личности, общества и государства. Сформированы теоретические основы данного вопроса. Однако, роль и место информационной безопасности в политической жизни общества и политическом курсе государства, направленном на защиту национальных интересов, требует дальнейшего осмысления.

Политика информационной безопасности Российской Федерации не может рассматриваться изолированно от долгосрочной стратегии развития информационного общества в стране. Развитие информационной сферы представляет собой важное направление политики модернизации российского государства. По поручению Президента России были разработаны основополагающие политически значимые документы: «Стратегия развития информационного общества» (Пр-212 от 07.02.2008)[1], «Доктрина информационной безопасности Российской Федерации» (Пр-1895 от 09.09.2000)[2].

Вопросы политики информационной безопасности регулярно обсуждаются на заседаниях Совета Безопасности Российской Федерации. При этом в авторитетном органе государственного управления Указом Президента Российской Федерации от 6 мая 2010 года № 590 создана Межведомственная комиссия по информационной безопасности[3].

В 2012-2013 гг. на официальном сайте Совета Безопасности Российской Федерации обнародованы «концепция Конвенции об обеспечении международной информационной безопасности», «Основные направления государственной политики Российской Федерации в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» и «Основы государственной политики Российской

[1] Российская газета, 2008, 16 февраля.
[2] Российская газета, 2000, 28 сентября.
[3] См.: Положение о межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности // Конституционно-правовой статус Совета Безопасности Российской Федерации / под общ. ред. . П. Патрушева. – 2-е изд., испр. и доп. – М.: Издательство «Известия», 2013. С. 263-266.

Федерации в области международной информационной безопасности до 2020 года»[4].

Таким образом, политика информационной безопасности, являясь важной составной частью политики национальной безопасности нашей страны, имеет комплексный характер и связана с основными сферами жизнедеятельности российского общества и геополитическими процессами в современном мире. В центре этой политики находится процесс обеспечения безопасности нашей страны в глобальном информационном пространстве.

С учетом вышеизложенного, актуальность избранной темы диссертационного исследования определяется следующими факторами:

1) Геополитическая ситуация вокруг Российской Федерации, становится все более сложной и нестабильной. Это связано с агрессивной, целенаправленной политикой США и других стран Запада по продвижению непосредственно к границам нашей страны военно-политических и экономических объединений. Подобные объединения вступают в непосредственную борьбу за влияние на государства постсоветского пространства с целью их интеграции в межгосударственные блоки и союзы, являющиеся прямыми геополитическими конкурентами России. В настоящее время события, связанные с украинским кризисом, еще раз наглядно подтверждают наличие серьезных угроз национальной безопасности нашей стране. В связи с этим, принципиальное значение имеет постоянный политологический анализ всего спектра угроз, исходящих из информационного пространства и возникающих в ходе обострения геополитической конкуренции в современном мире.

2) Превращение информационной составляющей в важнейшую часть всей системы национальной и ведущий элемент международной безопасности. Установка руководства Российского государства на развитие комплексной системы национальной безопасности, в которой информационной компоненте отводится роль ведущего звена и надежного щита для защиты интересов страны в глобальном пространстве, стимулирует развитие военно-политических и

[4] URL: http://www.scrf.gov.ru.

политологических исследований в области создания целостной теории национальной безопасности, включающей информационное измерение.

3) Обеспечение национальной безопасности в мирное время и в период военных действий в условиях современных войн в значительной степени зависит от результатов информационного противоборства, что настоятельно требует разработки эффективного механизма обеспечения информационной безопасности, как ведущего базового элемента всей системы национальной безопасности России. Такой механизм должен оптимально охватывать все основные аспекты защиты информационного пространства нашей страны, и в тоже время, быть инновационным, динамично развивающимися, чтобы оперативно реагировать как на новейшие достижения в информационно-коммуникационных технологиях, так и на трансформации, происходящие в современном глобальном мире. Деятельность по обеспечению информационной безопасности нашей страны непосредственно связана с геополитическими процессами в современном глобальном мире, с политическими проблемами международных отношений и нуждается в соответствующем обеспечении с позиций политической науки.

Степень научной разработанности темы исследования. В современной политической науке проблематика обеспечения национальной безопасности Российской Федерации в ее информационном измерении глобального мира изучена сравнительно мало. В раскрытии общетеоретических вопросов данной темы существенный вклад внесли в своих трудах А.Г. Арбатов[5], Д.Г. Балуев[6], И.И. Беляев[7], А.Д. Богатуров[8], А.В. Виноградов[9], А.В. Возженников[10], Н.В.

[5] Арбатов А.Г. Разоружение и безопасность2001-2002: Международная безопасность: новые угрозы нового тысячелетия / А.Г. Арбатов.- Рос. Акад. Наук, Ин-т мировой эконом. И междунар. Отношений, Центр геополит. И военных прогнозов.- М.: Наука, 2003.- 395с.

[6] Балуев Д. Г. Информационно-коммуникационные измерения политических процессов / Д. Г. Балуев и др.; под общ. ред. академика О. А. Колобова. – Н.Новгород: ННГУ, 2006.– 107 с.

[7] Беляев И. И. Предпосылки к формированию комплексной системы международной информационной безопасности: доклад [Электронный ресурс] / И. И. Беляев // Материалы 16-го Национального форума информационной безопасности «Инфофорум-2014», Москва 30-31 января 2014 г. – Режим доступа: http://2014.infoforum.ru/conference/programma/ (дата обращения: 16.05.2012)

[8] Богатуров А. Д. Россия в современной среде международной безопасности / А. Д. Богатуров // Россия в формировании международной системы профилактики распространения оружия массового поражения; отв. ред. А. А. Кокошин, А. Д. Богатуров. – М.: КомКнига, 2008. – С. 14-35.

[9] Виноградов А. В. Восток и Запад: ключи к политическим кодам / А. В. Виноградов // Мировые процессы. Журнал международной политики и международных отношений. – 2006. – Том 4. – № 1 (10). – С. 4-20.

[10] Возженников А. В. Национальная безопасность России: методология комплексного исследования и политика

Загладин[11], С.А. Караганов[12], О.Г. Карпович[13], А.А. Кокошин[14], Н.В. Косолапов[15], Ю.В. Косов[16], С.В. Кортунов[17], В.А. Кременюк[18], В.Н. Крутских[19], В.М. Кулагин[20], С.А. Ланцов[21], М.М. Лебедева[22], С.А. Модестов[23], С.А. Панкратов[24], И.В. Радиков[25], С.М. Рогов[26], С.В. Севастьянов,[27] А.В. Торопыгин[28], Н.И. Турко[29], А.И. Уткин[30], П.А. Цыганков[31], Т.А. Шаклеина[32], В.Л. Шульц[33], А.Ю. Шутов[34], Р.М.

обеспечения: монография / А. В. Возженников. – М.: Изд-во РАГС, 2002. – 423 с.

[11] Загладин Н.В. Стратегический глобальный прогноз, 2030: расширенный вариант / Н.В. Загладин.-Ин-т мировой экономики и междунар. Отношений РАН.- М:Магистр, 2011.-477с.

[12] Караганов С.А. «Глобальный ноль» и здравый смысл / С.А. Караганов // Россия в глобальной политике.-2010.-№3.- С. 108-118

[13] Карпович О. Г. Политика обеспечения национальной безопасности государства / О. Г. Карпович // Законы России: опыт, анализ, практика: профессиональный, тематический, юридический журнал. – 2012. – № 3. – С. 23-27.

[14] Кокошин А. А. Политико-военные и военно-стратегические проблемы национальной безопасности России и международной безопасности / А. А. Кокошин. – М.: Высшая школа экономики, 2013. – 261 с.

[15] Косолапов Н. В. Безопасность международная, национальная, глобальная: взаимодополняемость или противоречивость? / Н. В. Косолапов // Мировая экономика и международные отношения. – 2006. – № 9. – С. 3-13.

[16] Косов Ю. В. Некоторые особенности интеграционных процессов на евразийском пространстве (На примере ЕврАзЭС и ШОС) / Ю. В. Косов, А. В. Торопыгин // Евразийская интеграция: экономика, право, политика. – 2011. – № 10. – С. 157-165.

[17] Кортунов С. В. Мировая военно-политическая ситуация. Год 2025 / С. В. Кортунов // Международная жизнь. – 2010. – № 4. – С. 93-116..

[18] Кременюк В. А. Россия и США в новых международных условиях: асимметричное партнерство? / В. А. Кременюк. – М.: Ин-т США и Канады РАН, 2005. – 91 с.

[19] Крутских А. В. Политико-правовой режим глобальной информационной безопасности / А. В. Крутских // Современная мировая политика / Отв. ред. А.Д. Богатуров. – М.: Аспект-Пресс, 2009. – С. 484-485.

[20] Кулагин В.М. Современная международная безопасность / В.М. Кулагин.- М.: КноРус, 2012.- 431с.

[21] Ланцов С. А. Безопасность государства-общества-человека в контексте противодействия терроризму / С. А. Ланцов // Вестник Московского университета. Серия 12. Политические науки. – 2010. – № 4. – С. 58-62. Ланцов С. А. Теоретические концепции международной интеграции и перспективы интеграционных процессов на постсоветском пространстве / С. А. Ланцов // Вестник Санкт-Петербургского университета. Серия 6: Философия. Культурология. Политология. Право. Международные отношения. – 2013. – № 2. – С. 65-74.

[22] Лебедева М. М. Акторы современной мировой политики: тренды развития / М. М. Лебедева // Вестник МГИМО-Университета. – 2013. – № 3 (28). – С. 38-42.

[23] Модестов, С. А. Стратегическое сдерживание на театре информационного противоборства/ С. А. Модестов // Вестник Академии военных наук. – 2009. – № 1. – С. 33-36.

[24] Панкратов С. А. Глобальные и региональные факторы политического риска государственному режиму в условиях реализации национальной модели модернизации [Электронный ресурс] / С. А. Панкратов, И. М. Соколов // Теория и практика общественного развития. – 2012. – № 2. – Режим доступа: http://teoria-practica.ru/rus/files/arhiv_zhurnala/2012/2/politika/pankra-tov-sokolov.pdf (дата обращения: 16.03.2013)

[25] Радиков И. В. Политика и национальная безопасность: монография / И. В. Радиков. – СПб.: Астерион, 2004. – 348 с.

[26] Рогов С. М. Стратегическое одиночество России [Электронный ресурс] / С. М. Рогов // Экономические стратегии. – 2004. – № 4. – С. 12–17. – Режим доступа: http://www.tinlib.ru/istorija/besedy/p11.php. (дата обращения: 25.11.2012)

[27] Севастьянов С. В. «Новый регионализм» Восточной Азии: теоретические и практические аспекты / С. В. Севастьянов // Журнал «Полис»: Политические исследования. – 2009. – № 4. – С. 111-122.

[28] Торопыгин А.В. Парламентская дипломатия в структуре многосторонних международных отношений (На примере деятельности Постоянной комиссии МПА ЕврАзЭС по торговой политике и международному сотрудничеству)/ И.В. Карпенко, А.В. Торопыгин // Евразийская интеграция: экономика, право, политика № 7 - 2010.- С. 150-154

[29] Турко Н. И. Системология региональной безопасности. Геополитическое эссе / Н. И. Турко. – М., 2000.

[30] Уткин А. И. Мировая холодная война / А. И. Уткин. – М.: Эксмо, Алгоритм, 2005. – 736 с.

[31] Цыганков П.А. Универсальные ценности в мировой и внешней политике / П.А. Цыганков, Г.А.Дробот, В.А. Гуторов и др.; Под ред.П.А. Цыганкова. — М.: Издательство Московского университета, 2012. — 224 с.

[32] Шаклеина Т. А. Американские концепции статус-кво и современного миропорядка / Т. А. Шаклеина //

Юсупов[35], В.С. Ягья[36] и другие. Работы вышеперечисленных ученых посвящены анализу политических аспектов национальной и международной безопасности. В этих исследованиях анализируются философские и методологические основы изучения международной и национальной безопасности, значительное внимание уделяется раскрытию политических аспектов данного явления, его роли в эволюции мирового сообщества и развития нашей страны.

В последнее время повышается внимание к изучению проблем информационной безопасности, которая рассматривается как составная часть национальной безопасности и самостоятельный феномен[37]. В данной связи характерны труды таких авторов, как: В.К. Белозеров[38], М.В. Буйневич[39], Н.А. Васильева[40], М.А. Вус[41], М.А. Гареев[42], В.А. Гуторов[43], С.Б. Иванов[44], Л.Г. Ивашов[45], С.А. Комов[46], А.И. Коровянский[47], А.В. Лукин[48], И.Ф. Луппов[49], О.М.

Современная мировая политика. Под ред. А. Д. Богатурова. – М.: АСПЕКТ ПРЕСС, 2010. – С. 202-214.

[33] Шульц В. Л. Информационное управление в условиях активного противоборства: модели и методы / В. Л. Шульц, В. В. Кульба, А. Б. Шелков, Д. А. Кононов, И. В. Чернов. – М.: Наука, 2011. – 187 с.

[34] Шутов А. Ю. Современная цивилизация: вызовы и альтернативы / А. С. Капто, А. Ю. Шутов; под. ред. А. Ю. Шутова; Сер. Библиотека факультета политологии МГУ. – М.: Изд-во Московского государственного университета, 2013. – 304 с.

[35] Юсупов Р. М. Информационная безопасность и кибербезопасность: семантический конфликт и сосуществование / Р. М. Юсупов, В. М. Шишкин // Информатизация и связь. – 2013. – № 6. – С. 22-27.

[36] Ягья В. С. Балтинизация в контексте глобализации и регионализации мировой политики / В. С. Ягья // Россия и мир: опыт и проблемы модернизации. – СПб.: СПбГУТД, 2011. – С. 304-309

[37] Научные и методологические проблемы информационной безопасности (сборник статей) / Под ред. В. П. Шерстюка. – М.: МЦНМО, 2004. – 208 с.

[38] Белозёров В. К. Стратегия национальной безопасности Российской Федерации до 2020 года: проблемы реализации: монография / В. К. Белозёров и др. – М.: Издательский дом «АТИСО», 2011.

[39] Буйневич М. В. Организационно-техническое обеспечение устойчивости функционирования и безопасности сети связи общего пользования / М. В. Буйневич, А. Г. Владыко, С. М. Доценко, О. А. Симонина. – СПб.: Изд-во СПбГУТ, 2013.– 144 с.

[40] Васильева Н. А. К вопросу о формировании внешнеполитической стратегии РФ / Н. А. Васильева // Актуальные проблемы мировой политики: сборник научных трудов. Выпуск 2; сост. В. С. Ягъя. – СПб.: Нестор-История, 2007.

[41] Вус М.А. Информатика: Введение в информационную безопасность / М.А. Вус, В.С. Гусев, Д.В. Долгирев, А.А. Молдовян – СПб.: Изд-во «Юридический центр Пресс», 2004.-216 с. Вус М.А. В интересах национальной и международной информационной безопасности / М.А. Вус, О.С. Макаров // Информатизация и связь.-2013.- № 6.

[42] Гареев М. А. Стратегическое сдерживание - важнейшее направление обеспечения национальной безопасности России в современных условиях / М. А. Гареев // Стратегическая стабильность. – 2009. – № 1. – С. 2-13.

[43] Гуторов В. А. К вопросу о происхождении государства: парадоксы и аномалии современных интерпретаций / В. А. Гуторов // Журнал «Полис». Политические исследования. – 2014. – № 3. – С. 91-110.

[44] Иванов, С. Б. Вооруженные силы России и ее геополитические приоритеты / С. Б. Иванов // Россия в глобальной политике. – 2004. – № 1. – С. 36

[45] Ивашов, Л. Г. Россия или Московия? Геополитическое измерение национальной безопасности России / Л. Г. Ивашов. – М.: Изд-во «Эксмо», 2002. – 416 с.

[46] Комов С. А. Термины и определения в области информационной безопасности / С. А. Комов, В. В. Ракитин, С. Н. Родионов С. Н. [и др.]. – М.: Издательство «АС-Траст», 2009. – 304 с.

[47] Коровянский А. И. Военная безопасность Российской Федерации и ее обеспечение в современных условиях / А. И. Коровянский. – М.: Изд-во РАГС, 2010. – 218 с.

[48] Лукин А. В. Шовинизм или хаос: порочный выбор для России / А. В. Лукин // Журнал Полис: Политические исследования. – 2014. – № 3. – С. 159-172.

Михайленок[50], К.А. Панцирев[51], В.С. Пирумов[52], А.В. Понеделков[53], Д.О. Рогозин[54], А.С. Сергунин[55], В.И. Слипченко[56], А.А. Стрельцов[57], О.Ф. Шабров[58], Д.Н. Шакин[59], Е.Б. Шестопал[60] и другие. Исследования указанных авторов в основном посвящены изучению политики в сфере обеспечения информационной безопасности и ее влиянию на обороноспособность государства, анализу политико-правовых аспектов обеспечения национальной и информационной безопасности, определению влияния военной стратегии и военного искусства на поддержание безопасности, выявлению экономических, институциональных и социально-культурных основ безопасности и др. В отечественных исследованиях до настоящего времени уделялось мало внимания информационному измерению политики национальной безопасности, что не дает возможности экспертному сообществу проводить целенаправленное и всестороннее изучение информационного направления обеспечения национальной безопасности России.

Большое значение для осмысления и углубленного анализа проблем национальной безопасности имеют научные труды, связанные с изучением

---

[49] Луппов И. Ф. Современный терроризм как политический феномен / И. Ф. Луппов // Известия Российского государственного педагогического университета им. А.И.Герцена. – 2009. – № 103. – 225-231.

[50] Михайленок О. М. Стратегическая культура как системообразующий фактор общественно-политического согласия / О. М. Михайленок // Россия реформирующаяся. Выпуск 11: Ежегодник / Отв. ред. М. К. Горшков. – М.: Новый хронограф, 2012. – С. 125-141.

[51] Панцерев К.А. Информационное общество: эволюция концепции в исторической перспективе / К. А. Панцерев // Вестник Санкт-Петербургского Университета. Серия 6. Философия. Культурологи. Политология. Право. Международные отношения. – 2010. – Вып.1. – С. 65-72.

[52] Пирумов В. С. Информационное противоборство. Четвертое измерение противостояния / В. С. Пирумов. – М.: «Оружие и технологии», 2010. – 252 с.

[53] Понеделков В. В. Региональные административно-политические элиты России: итого постсоветской эволюции / В. В. Понеделков, В. Д. Лысенко // Социология власти. – 2012. – № 3. – С. 30-39.

[54] Рогозин Д. О. Свой чип карман не тянет / Д. О. Рогозин // Российская газета. – 2014. – 15 августа. – № 184(6456). – С. 5.

[55] Сергунин А. А. Суверенитет: современные дискуссии в теории международных отношений / А. А. Сергунин // Научные ведомости Белгородского госуниверситета. Серия История. Политология. Экономика. Информатика. – 2010. – № 19(90). – Выпуск 16. – С. 231-236.

[56] Слипченко В. И. Информационное противоборство в бесконтактных войнах [Электронный ресурс] / В. И. Слипченко. – Режим доступа http://viperson.ru/wind.php?ID=291897&soch=1. (дата обращения: 11.04.2013)

[57] Стрельцов А. А. Обеспечение информационной безопасности России. Теоретические и методологические основы / А. А. Стрельцов: из серии монографий под общ. ред. В. А. Садовничего и В. П. Шерстюка «Научные проблемы безопасности и противодействия терроризму». – М.: МЦНМО, 2002. – 86 с.

[58] Шабров О. Ф. Государство в глобализующемся мире: испытание постмодерном / О. Ф. Шабров // Власть и политика: институциональные вызовы XXI века. Политическая наука: Ежегодник 2012 / Российская ассоциация политической науки; гл. ред. А. И. Соловьев. – М.: Российская политическая энциклопедия (РОССПЭН), 2012. – С. 87-101.

[59] Шакин Д. Н. Информационная безопасность: коллективная монография / Д. Н. Шакин (руководитель), Е. Г. Бунев, С. М. Доценко, В. С. Пирумов, С. И. Тынянкин и др. – М.: Оружие и технологии, 2009. – 264 с.

[60] Шестопал Е. Б. Образы государств, наций и лидеров / Е. Б. Шестопал. – М.: Аспект Пресс, 2008. – 288 с.

вопросов информационного измерения безопасности в контексте проблем развития глобального мира и процессов глобализации. Данные вопросы поднимают в своих работах В.А. Ачкасов[61], С.М. Виноградова[62], С.Г. Еремеев[63], В.П. Кириленко[64], А.И. Смирнов[65], К.К. Худолей[66] и другие.

Достаточно большой массив исследований посвящен анализу информационного противоборства в современном мире, особенностям ведения информационных войн, функционированию и перспективам развития средств и сил обеспечения информационной безопасности. Данное направление развивают: Е.В. Бродовская[67], В.М. Буренок[68], А.А. Вилков[69], П.С. Золотарев[70], Н.Н. Извеков,[71] Н.А. Комлева[72], И.М. Левкин[73], А.В. Манойло[74], А.С. Пую[75], В.М Смирнов[76], С.А. Суханов[77], Д.Б. Фролов[78], Б.Ф. Чельцов[79], С.А. Шомова[80] и другие.

---

[61] Ачкасов В. А. Кризис национальной идентичности и проблемы безопасности России / В. А. Ачкасов // Вестник Московского университета. Серия 12. Политические науки. – 2010. – № 4. – С. 63-67.

[62] Виноградова С. М. Государство в современной информационно-политической системе / С. М. Виноградова, Г. С. Мельник // Вестник Санкт-Петербургского университета. Серия 9: Филология. Востоковедение. Журналистика. – 2007. – № 4-1. – С. 115-131.

[63] Еремеев С. Г. К проблеме актуализации политической власти как ценности в эпоху глобализации / С. Г. Еремеев // Вестник Московского университета. Серия 12. Политические науки. – 2012. – № 3. – С. 52-54.

[64] Кириленко В. П. Современный терроризм – глобальная угроза человечеству / В. П. Кириленко, А. Ю. Пиджаков. – СПб.: Изд-во Политехн. ун-та, 2008. – 464 с.

[65] Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности / А.И. Смирнов.- М.: ПАРАД, 2005.- 391с.

[66] Худолей К.К. Россия и европейская интеграция: прошлое, настоящее, будущее /К.К. Худолей.-Спб: Издательство СПБГУ, 2012.- 332с.

[67] Бродовская Е. В. Политические функции Интернета в восприятии россиян / Е. В. Бродовская, В. Д. Нечаев // Городское управление. – 2013. – № 8. – С. 89-95.

[68] Буренок В. М. О некоторых аспектах информационных войн / В. М. Буренок // Вооружение и экономика. – 2011. – № 3(15). – С. 5-16.

[69] Вилков А. А. Политическая функциональность современных российских СМИ / А. А. Вилков, С. Ф. Некрасов, А. В. Россошанский. – Саратов: Изд-во «Научная книга», 2011. – 268 с.

[70] Золотарев П.С. Цели и приоритеты военной политики России / П.С. Золотарев // Россия в глобальной политике.- 2007.- №2.- С. 76-87

[71] Извеков Н.Н. Проблема ограничения вооружений в XXI веке / Н.Н. Извеков // Обозреватель.-2008.-№2.-С. 74-81

[72] Комлева Н. А. Интернет как ресурс сетевой войны [Электронный ресурс] / Н. А. Комлева, Г. Саймонс, Д. Л. Стровский // Журнал ПОЛИТЭКС. – 2010. – № 2. – Режим доступа: http://www.politex.info/content/view/72. (дата обращения: 8.10.2013)

[73] Левкин И. М. Основные проблемы информационно-экономической безопасности Российской Федерации на современном этапе / И. М. Левкин, С. Ю. Микадзе // VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2013 г.: Материалы конференции / СПОИСУ. – СПб., 2013. – С. 176-177.

[74] Манойло А.В, Модели информационно-психологического управления международными конфликтами / А.В. Манойло // Вестник Моск. Ун-та. Серия 12. Политические науки.-2012.-№2.- С. 85-95

[75] Пую А. С. Информационные технологии и терроризм: теория и современная практика / А. С. Пую, Н. С. Лабуш, А. Ю. Евсеев. – СПб.: Роза мира», 2005. – 147 с.

[76] Смирнов В. М. Космос в вопросах сооруженной борьбы / В. М. Смирнов // Национальная оборона. – 2008. – №7.

[77] Суханов С. А. Угрозы безопасности России растут. Роль и место ракетно-космической обороны страны в парировании возможного нападения / С. А. Суханов, В. П. Омельчук, В. Ф. Фатеев // Воздушно-космическая оборона. – 2006. – №4(29). – С. 28-31.

Однако, круг работ, посвященных теоретическому анализу и обобщению проблем обеспечения национальной безопасности в информационном измерении, еще весьма ограничен. С одной стороны, они порой «рассеяны» и скрыты в контексте общих практических вопросов деятельности государства в данной сфере, а с другой – проводится анализ только отдельных аспектов обеспечения национальной безопасности в глобальном информационном пространстве. Развитие современной ситуации в данной сфере поставило на повестку дня вопрос о проведении целостного комплексного исследования обеспечения национальной безопасности России в глобальном информационном пространстве.

Объектом исследования является национальная безопасность Российской Федерации, изучаемая в условиях современного глобального мира.

Предмет исследования – информационная компонента состояния национальной безопасности России в глобальном информационном пространстве в контексте современной геополитической ситуации.

Цель исследования – разработать концептуальные подходы по формированию политики модернизации системы национальной безопасности Российской Федерации в условиях современного глобального развития на основе анализа влияния информационных факторов на сферу национальной безопасности страны.

Данная цель была конкретизирована в диссертационном исследовании путем постановки ряда **научных задач**, наиболее важными из которых являются:

- политологический анализ состояния проблемы национальной безопасности Российской Федерации в контексте глобальных политических процессов современного мира;

---

[78] Фролов Д. Б. Информационная геополитика и вопросы информационной безопасности / Д. Б. Фролов // Национальная безопасность. – 2009. – № 1. – С. 72–79.

[79] Чельцов Б. Ф. Вопросы воздушно-космической обороны в военной доктрине России / Б. Ф. Чельцов // Военная мысль. – 2007. – №4. – С. 5-10.

[80] Шомова С. А. СМИ или медиа? (К вопросу об определении понятий) / С. А. Шомова, Т. Б. Тихомирова // Россия: на пути глобализации и интеграции: Научные труды ИМПЭ им. А.С. Грибоедова. К 20-летию Института международного права и экономики имени А. С. Грибоедова. Вып. 2012. – М.: Издательский дом «Буквовед», 2012. – С. 260-264.

− совершенствование и развитие концептуального аппарата политологического исследования национальной безопасности в информационном измерении;

− исследование влияния военно-политической глобализации на сферу национальной безопасности России;

− обоснование комплекса мер для модернизации системы национальной безопасности Российской Федерации в контексте повышения значимости информационной составляющей в современных условиях;

− оценка влияния политики информационной безопасности на обеспечение национальной безопасности Российской Федерации;

− выявление специфики глобального информационного противоборства на мировой арене в условиях новейших геополитических трансформаций;

− раскрытие особенностей обеспечения информационной безопасности Российского государства на региональном уровне.

Методология исследования. Общеметодологической основой исследования выступает диалектический метод познания, применяемый для проведения теоретического анализа в политической науке. В ходе диссертационного исследования автор использует принципы развития, связи, универсальности, системности, комплексности, фундаментальные положения политической науки о международных отношениях, глобальном и региональном развитии, формах и политических способах обеспечения национальной безопасности. В качестве методологических подходов, имеющих частный характер, использованы положения политической науки относительно национальной и информационной безопасности, значимые для темы диссертационного исследования: принципы информационного противоборства, методы ведения информационной войны, критерии информационной культуры и др. Специализированными теоретико-методологическими предпосылками послужили труды отечественных и зарубежных авторов, посвященные вопросам изучения геополитики, процессов глобализации, национальной и информационной безопасности государства и общества. Таким образом,

исследование было осуществлено с применением как общетеоретических, так и частных политологических методов и методологических подходов.

Собственно исследовательский инструментарий диссертации, который формирует ее концепцию, составили два взаимодополняющих друг друга подхода. Первый подход – аналитико-констатирующий. Он основан на признании противоречия между требованиями геополитических реалий к построению оптимальной системы обеспечения национальной безопасности Российской Федерации в глобальном информационном пространстве и складывающейся практикой ее функционирования. Второй подход – вероятностно-прогностический. В его основе лежит гипотеза о том, что одним из возможных путей преодоления данного противоречия является формирование политики модернизации системы национальной безопасности с учетом политических особенностей ее функционирования в глобальном информационном пространстве.

Эмпирическая база исследования опирается на данные политологических исследований, национальные и международные нормативно-правовые акты, акты Президента Российской Федерации, нормативные документы Федерального Собрания Российской Федерации, постановления и распоряжения Правительства Российской Федерации, материалы и документы Совета Безопасности России и других государственных органов. В работе нашли применение широкий круг статистических данных и аналитических материалов, экспертных оценок ведущих специалистов в области национальной и информационной безопасности, отечественных и зарубежных информационных источников, относящихся к исследуемой проблематике.

Научная новизна работы.

1) Впервые сформулирован и применен всесторонний подход к учету влияния тенденций в глобальном информационном пространстве по обеспечению политики национальной безопасности.

2) По-новому структурирована проблема комплексного решения задачи обеспечения информационной безопасности России.

3) Обоснована современная характеристика информационного противоборства с позиции политической науки: раскрыты политические цели, основные черты и формы проявления данного глобального процесса.

4) Предложена авторская интерпретация феномена военно-политической глобализации, как ключевого фактора в процессе модернизации системы национальной безопасности России.

5) В научный оборот введен ряд новых, не представленных ранее в российской научно-политической литературе понятий, отражающих явления интеграции политических и информационных процессов в сфере национальной безопасности.

6) Рассмотрен сценарный прогноз развития сети Интернет в среднесрочной перспективе в контексте политики модернизации системы национальной безопасности России.

7) Определены новые категории в политической науке, необходимые для анализа информационно-политических аспектов национальной безопасности.

8) Разработаны методики квалиметрических оценок в политических науках для определения возможного ущерба национальной безопасности в информационном пространстве.

9) Проведено ранжирование угроз национальной безопасности в глобальном информационном пространстве.

10) Впервые раскрыты политические аспекты культуры информационной безопасности.

11) Исследовано современное состояние асимметрии между ведущими мировыми державами в глобальном информационном пространстве и предложены рекомендации по реализации политики России в данных условиях.

12) Разработаны и обоснованы основные направления формирования и реализации системы мер по обеспечению региональной политики информационной безопасности для международного (на примере государств – членов ОДКБ) и внутреннего (на примере Северо-Западного федерального округа России) регионов.

На защиту выносятся следующие положения, обладающие научной новизной и конкретизирующие концепцию диссертации.

1) Как показал проведенный анализ, взаимозависимость государств и регионов мира в период обострения глобальных проблем, имеющих политическую, экономическую, экологическую, энергетическую и иную природу, выдвинули на первый план проблему обеспечения национальной безопасности.

Для процессов обеспечения национальной безопасности в современных условиях характерны следующие тенденции:

− повышение значимости информации и знаний для поддержания безопасности;

− увеличение доли информационных коммуникаций, средств и продуктов программного обеспечения, используемых в процессе обеспечения безопасности;

− зависимость современного прогресса в сфере защиты национальной безопасности от успехов развития информационных технологий и связанных с ним областей экономики и финансов;

− появление новых угроз информационной безопасности из глобального информационного пространства, которое имеет планетарный масштаб охвата.

В данной связи политика национальной безопасности Российской Федерации в современных тенденциях глобального информационного пространства носит всесторонний характер и направлена на:

− договоренность с основными державами мира по предотвращению и урегулированию локальных и региональных вооруженных конфликтов через миротворчество, принуждение к миру, борьбу с международным терроризмом и наркоторговлей;

− взаимодействие по пресечению распространения ядерного оружия и других видов оружия массового уничтожения, усиление режимов экспортного контроля и ужесточение санкций к их нарушителям;

− сотрудничество великих держав по созданию единой системы ПРО с использованием сил и средств ВКО России, интенсификацию переговоров по

сокращению обычных вооружений, неприменению в вооруженных конфликтах оружия, наносящего массовое поражение личному составу;

− объединение усилий по предотвращению кризисных явлений во всех сферах человеческой деятельности с использованием современных информационных технологий.

2) Повышение статуса Российской Федерации в международном сообществе требует от нашей страны развиваться такими же инновационными темпами, как и другие великие державы и высокоразвитые индустриальные государства, а на некоторых направлениях и опережать их, уделяя особое внимание обеспечению информационной безопасности как базовому элементу системы национальной безопасности страны. Решение этой задачи следует осуществлять комплексно, на трех главных уровнях обеспечения информационной безопасности: отраслевом, национальном и международном. На первом уровне должно быть обеспечено устойчивое функционирование информационной инфраструктуры. Второй – связывает между собой всю основу национальной безопасности страны. На третьем – необходимо предотвращать возникновение угроз из глобального информационного пространства и обеспечивать информационно-политическую, информационно-технологическую и информационно-психологическую сферы национальной безопасности.

3) Информационное противоборство, порождаемое обостряющейся конкуренцией между ведущими державами современного мира, все в большей мере будет распространяться на российское информационное пространство. В ходе глобального информационного противоборства государство преследует следующие политические цели: модернизация системы национальной безопасности; защита и продвижение национальных интересов в информационной сфере; обеспечение информационной безопасности как важного элемента национальной безопасности; укрепление международной безопасности; создание и применение отечественных высоких технологий.

Информационная мощь ведущих держав современного мира позволяет им реализовывать свои важные геополитические цели в некоторых случаях без применения силовых инструментов.

В диссертационной работе дана характеристика глобального информационного противоборства, которому присущи следующие основные черты: скрытый, неявный характер осуществления; высокая скорость распространения информации; реализация многих действий при широкомасштабном использовании средств массовой информации и сети Интернет; действия в рамках глобального информационного пространства. В этой связи серьезную опасность представляет информационный терроризм, как составная часть международного терроризма, активно действующего в глобальном информационном пространстве, не признавая государственных границ, не имея ни национальной, ни религиозной принадлежности.

Основными формами информационного противоборства могут быть: информационное доминирование; информационная асимметрия; информационное сдерживание; информационная агрессия.

4) В настоящее время глобализация превратилась в основную тенденцию мирового развития, оказывает самое существенное влияние на военно-политическую сферу и повышает значимость информационной безопасности на национальном уровне. Это влияние многоплановое и противоречивое, как и сам процесс глобализации. Во-первых, государство с хорошо подготовленными и оснащенными вооруженными силами, при условии жесткого противостояния в глобальном мире, способно защитить свои национальные интересы. Во-вторых, военно-политическая глобализация дала толчок развитию инновационных технологий, которые позволили создать новые современные виды вооружений и новые рода войск: информационные или кибервойска. В-третьих, глобализация привела к расширению сфер боевого применения – военные действия планируются в глобальном информационном пространстве и в космосе.

Современные военные конфликты в качестве театра военных действий включают в себя, в том числе, и информационное пространство конфликтующих

сторон. Кроме того, военные конфликты порождают информационные войны в глобальном мире. Следует также отметить, что военно-политическая глобализация выступает ключевым фактором модернизации всей системы национальной безопасности Российской Федерации.

5) В ходе диссертационного исследования обоснован ряд новых понятий политической науки, необходимых для теоретического изучения и разработки практических рекомендаций по обеспечению национальной безопасности в информационно-политическом измерении:

– информационно-политическая безопасность – это состояние защищенности государства, при котором обеспечивается политика информационной безопасности в условиях существующих угроз из глобального информационного пространства с использованием СМИ, сети Интернет и других средств распространения информации;

– информационно-политическая устойчивость – это способность государства осуществлять политику нейтрализации существующих угроз в информационном пространстве с целью обеспечения безопасности в информационно-политической, информационно-технологической и информационно-психологической сферах системы национальной безопасности страны;

– информационно-политический кризис – это общественно-политическое явление, для которого характерны перенос политической борьбы в информационную сферу и использование в политических конфликтах средств информационного противоборства, что порождает возникновение серьезных негативных последствий для национальной безопасности государства.

В работе также были сформулированы и другие понятия, необходимые для раскрытия темы исследования (информационно-политическая необходимость, информационно-политическая достаточность, информационно-политический консенсус).

6) Предотвращение или парирование угроз возникающих в информационном пространстве выступают в качестве важных факторов для

обеспечения национальной и международной безопасности. Такой подход особенно важен, когда сеть Интернет постепенно превратилась в важный политический ресурс влияния на общественное сознание. Этому способствовали следующие особенности данной сети как средства коммуникации: всемирный масштаб охвата, высокая скорость распространения политической информации, мультимедийность, интерактивность.

Интернет-ресурсы также активно используются в преступных целях: кибертерроризм, размещение порнографического контента или контента, содержащего информацию о наркотиках, информацию, побуждающую к самоубийствам («киберсуицид») и т.п.

При проведении политики модернизации системы национальной безопасности России необходимо принимать во внимание три возможных сценария развития Интернета в среднесрочной перспективе: первый – сохранение статус-кво в этой глобальной системе; второй – распад глобальной сети на региональные и национальные системы гораздо меньших масштабов и обособленные друг от друга различными защитными и контрольными структурами; третий – создание индустриально развитыми государствами современного мира защищенных национальных информационно-коммуникационных сетей, которые допускают выход информационного контента, не представляющего угрозу национальной безопасности, в глобальную сеть.

7) В результате исследования национальной безопасности в информационно-политическом измерении предложено ввести в политическую науку новые категории:

– информационный суверенитет – это верховенство и независимость государственной власти при формировании и реализации информационной политики. Верховенство реализуется в национальном сегменте, а независимость – в глобальном информационном пространстве. В диссертации раскрыты основные сферы проявления информационного суверенитета, а именно: информационно-технологическая, информационно-психологическая, информационно-политическая. Впервые в политической науке представлена структура

информационного суверенитета, включающая в себя следующие основные элементы: цифровой, ментальный и властный суверенитеты;

– государственная политика информационного суверенитета – это деятельность государства по осуществлению самостоятельной информационной политики на основе существующих законов страны и норм международного права в информационной сфере с целью обеспечения информационной безопасности личности, общества и государства.

8) В диссертационном исследовании разработаны и предложены для мониторинга системы национальной безопасности критерии и показатели оценки возможного ущерба государству в информационном пространстве. Для анализа изучаемых в диссертации процессов, автором разработаны методики квалиметрических оценок: методика регрессивного анализа ущерба; методика нахождения квалиметрических показателей на основе линейных сверток для комплексных количественных оценок в политических науках; методика оценки возможного ущерба государству из вероятностной модели событий.

9) При анализе концептуальных основ политики национальной безопасности сделан вывод, что одной из центральных категорий является «угроза национальной безопасности». На первый план в современной международной политике выходят новые вызовы и угрозы, имеющие трансграничную природу. Среди них по масштабам проявления, степени диверсификации, возможному ущербу и последствиям выделяются угрозы национальной безопасности в информационном пространстве. В диссертационном исследовании произведена классификация данных угроз по следующим факторам: по компонентам информационной сферы, по расположению источника угроз, по происхождению угроз, по характеру деструктивного воздействия, по целям воздействия, по масштабам проявления. Проведен анализ основных выделенных групп типовых угроз.

10) Выявлены причины, обуславливающие необходимость формирования культуры информационной безопасности, раскрыто содержание данной культуры и проанализированы ее составные элементы: осведомленность, ответственность,

риск-менеджмент, реагирование и др. Разработаны рекомендации по формированию культуры информационной безопасности общества.

11) В отношениях России с США и НАТО в информационной сфере сложилась асимметрия, причины которой имеют политическую, идеологическую, экономическую и технологическую природу. В данных условиях нашей стране следует искать адекватные ответы на потенциальные информационные угрозы с Запада. Следует сосредоточить активность в информационном пространстве тех регионов, где особенно важны наши национальные интересы. Для обеспечения национальной безопасности Российской Федерации в информационной сфере перспективным направлением является сотрудничество в рамках ОДКБ, ШОС, БРИКС.

12) В ходе исследования деятельности органов власти государств – членов ОДКБ были разработаны и обоснованы основные направления обеспечения региональной политики информационной безопасности:

– формирование общего информационного пространства безопасности, как объединенного сегмента информационных пространств государств – членов ОДКБ;

– сближение и гармонизация законодательств стран Организации.

Предложена система мер по реализации региональной информационной политики:

– унификация понятийного аппарата в сфере обеспечения информационной безопасности;

– политико-организационные мероприятия совместной деятельности по обеспечению информационной безопасности в рамках ОДКБ;

– синхронизация существующих и создание новых единых технологических стандартов для обеспечения информационной безопасности.

Автором разработана и реализована на практике система защиты информации в Северо-Западном федеральном округе, обеспечивающая координацию деятельности федеральных, региональных органов государственной власти и органов местного самоуправления, а также предприятий оборонно-

промышленного комплекса. В диссертации предложена «Концепция политики информационной безопасности в Северо-Западном федеральном округе», в основу которой положена государственная политика информационного суверенитета на региональном уровне.

Теоретическая значимость исследования заключается в концептуализации и систематизации основных теоретических положений по обеспечению национальной безопасности Российской Федерации во всемирном информационном пространстве в условиях становления новой архитектуры глобальной безопасности. В работе введены новые понятия и категории политической науки, позволяющие расширить и углубить возможности теоретического осмысления информационной составляющей национальной безопасности в условиях современных политических процессов глобального развития.

Практическая значимость. Полученные в диссертации результаты и выводы были использованы в деятельности Экспертно-консультативного совета, членом которого является автор, при Совете Парламентской Ассамблеи ОДКБ и Парламентских комиссий МПА СНГ при разработке документов: «Рекомендаций по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере информационной безопасности» (принят МПА СНГ 23 ноября 2012 года Постановлением № 3820); «Рекомендаций по правовому регулированию эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в террористических и иных противоправных целях», (принят МПА СНГ 29 ноября 2013 года Постановлением № 3923); «Рекомендаций по сближению и гармонизации законодательства государств – членов ОДКБ по защите государственных секретов» и Глоссария основных понятий в законодательстве о государственной тайне государств – членов ОДКБ (принят Парламентской Ассамблеей ОДКБ 27 октября 2010 года Постановлением № 4-7).

Результаты диссертационного исследования используются в настоящее время при подготовке проектов «Стратегии обеспечения информационной

безопасности государств – участников СНГ», Модельного регламента административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности государств – участников СНГ, Модельного закона «О критически важных объектах информационно-коммуникационной инфраструктуры» и при разработке изменений в модельный закон «Об информации, информатизации и защите информации».

Соответствующие положения диссертации были применены автором при разработке дополнений к «Концепции политики информационной безопасности в Северо-Западном федеральном округе до 2015 года», которые были утверждены Межведомственным советом по защите информации при полномочном представителе Президента Российской Федерации в Северо-Западном федеральном округе 17 декабря 2010 года.

Материалы диссертации были использованы в учебном процессе в Северо-Западном институте управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации и других ВУЗах страны и в том числе при подготовке учебно-методических комплексов: «Теоретические проблемы национальной безопасности», «Информационная безопасность в современных международных отношениях», «Содружество Независимых Государств», «ООН и международная интеграция», «Политология» и др.

Степень достоверности и апробация результатов исследования. Степень достоверности результатов, полученных автором диссертационной работы, определяется использованием признанных научных методов исследования и опорой на обширный эмпирический материал, включающий в себя: нормативно-правовые акты органов государственной власти, материалы политологических исследований и труды ведущих российских и зарубежных ученых и др.

Диссертация обсуждена и рекомендована к защите на заседании кафедры международных отношений Северо-Западного института управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации.

Основные положения диссертации **докладывались** и **обсуждались** на:

- Всероссийской научно-практической конференции «Проблемы обеспечения геополитической безопасности России», Екатеринбург, 24-25 сентября 2009 г.;
- Международной научной конференции к 200-летию со дня основания Императорского Царскосельского лицея «Императорский Царскосельский лицей в истории России XIX-XXI вв.», Санкт-Петербург, 20-21 октября 2011 г.;
- VII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2011)», Санкт-Петербург, 26-28 октября 2011 г.;
- Международной научно-практической конференции «Право на доступ к информации: возможности и ограничения в электронной среде», Санкт-Петербург, Президентская библиотека имени Б. Н. Ельцина, 13 апреля 2012 г.;
- 4-ой научно-практической конференции «Информационная безопасность. Невский диалог – 2012», Санкт-Петербург, ЛЕНЭКСПО, 23-24 октября 2012 г.;
- Юбилейной XIII Санкт-Петербургской Международной конференции «Региональная информатика (РИ-2012)», Санкт-Петербург, 24-26 октября 2012 г.;
- Международной научной конференции – пятых Санкт-Петербургских социологических чтениях «Социология безопасности: проблемы, анализ, решения», Санкт-Петербург, 19-20 апреля 2013 г.;
- XXII ежегодном Российско-американском семинаре «Грядущий мировой порядок в оценках российских и американский экспертов», Санкт-Петербург, Санкт-Петербургский государственный университет, 15-21 мая 2013 г.;
- IV Всероссийской научно-технической конференции «Проблема комплексного обеспечения информационной безопасности и совершенствование образовательных технологий подготовки специалистов силовых структур», Санкт-Петербург, 10-11 октября 2013 г.;
- VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013)», Санкт-Петербург, 23-25 октября 2013 г.;

– Международной научно-практической конференции «Евразийский регион в глобальной архитектуре современного мира», Санкт-Петербург, МПА Евразийского экономического сообщества – СЗИУ РАНХиГС, 24-25 октября 2013 г.;

– Международной научно-практической конференции «Законодательство государств-членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности: опыт, проблемы и перспективы гармонизации», Санкт-Петербург, Межпарламентская ассамблея государств-участников Союза Независимых Государства – Парламентская Ассамблея Организации Договора о коллективной безопасности, 28 ноября 2013 г.;

– II российско-китайском экономическом форуме «Современные российско-китайские экономические отношения: инновационный вектор развития», Санкт-Петербург, Северо-Западный институт управления – филиал РАНХиГС, 26 мая 2014 г.;

– Международной научно-практической конференции «Чрезвычайное законодательство и образование в условиях глобализации», Санкт-Петербург, СПбУГПС МЧС России, 28-29 мая 2014 г.;

– Международной научной конференции «Единство власти, культуры, образования и науки – путь к успешному обществу», Санкт-Петербург, СЗИУ РАНХиГС, 17 июня 2014 г.;

– Заседаниях Межведомственного совета (МВС) по защите информации при полномочном представителе Президента Российской Федерации в Северо-Западном федеральном округе, Санкт-Петербург: МВС-12 (2 декабря 2009 г.), МВС-13 (7 декабря 2010 г.), МВС-14 (14 декабря 2011 г.), МВС-15 (4 декабря 2012 г.), МВС-16 (13 декабря 2013 г.);

– Совещании с высшим руководящим составом Северо-Западного федерального округа: «О состоянии технической защиты информации в Северо-Западном федеральном округе в 2009 году», Санкт-Петербург, 26 марта 2010 г.;

– Совместном заседание Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности и секции

по информационной безопасности научного совета при Совете Безопасности Российской Федерации, Москва, 14 декабря 2010 г.;

– Расширенных заседаниях Совета по вопросам безопасности, противодействию коррупции и экстремизму при полномочном представителе Президента Российской Федерации в Северо-Западном федеральном округе, Санкт-Петербург (15 апреля 2011 г., 28 сентября 2012 г., 28 февраля 2013 г., 19 апреля 2013 г., 26 апреля 2013 г., 7 августа 2013 г., 16 октября 2013 г., 19 ноября 2013 г., 17 апреля 2014 г.)

– Заседаниях Экспертно-консультативного совета при Совете Парламентской Ассамблеи ОДКБ, Санкт-Петербург (16 мая 2012 г., 10 апреля 2013 г., 15 апреля 2014 г.);

– Заседаниях Объединенной комиссии МПА СНГ по гармонизации законодательства в сфере борьбы с терроризмом, преступностью и наркобизнесом, а также противодействия новым вызовам, Санкт-Петербург (26-27 февраля 2013 г., 17-18 апреля 2014 г.);

– Заседании Ученого Совета Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН), Санкт-Петербург, 9 июня 2014 г.

Основные результаты диссертационного исследования опубликованы в 29 статьях в научных журналах (из них 22 – из Перечня ВАК), в четырех монографиях (из них 3 – лично) и двух словарях-справочниках, а также в 13 сборниках материалов конференций.

1. ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ В АСПЕКТЕ ГЛОБАЛЬНЫХ ПОЛИТИЧЕСКИХ ПРОЦЕССОВ СОВРЕМЕННОГО МИРА

В наше время стало возможным говорить о формировании мирового информационного пространства. Это пространство представляет собой глобальную информационно-коммуникационную сеть, связывающую миллиарды пользователей на разных континентах, во всех, даже самых удаленных, уголках нашей планеты. Так, по данным на середину 2012 г., в мире насчитывались 2 405 518 376 пользователей Интернета (для сравнения: в 2000-м их число составляло всего 360 985 492 чел.). Среди пользователей Всемирной информационной паутиной больше всего китайских граждан – 22,4%, на втором месте идут представители США – 10,2%; россияне занимают шестое место: в Глобальной информационной сети их – 2,8%[81].

Все активнее в мировое информационное пространство включаются государственные учреждения, негосударственные организации и социальные институты, представляющие все основные сферы жизнедеятельности общества, а также широкие массы индивидуальных участников информационно-коммуникационных процессов.

Основой процесса создания такого пространства следует рассматривать переход человечества от индустриального общества к обществу знаний, в котором информационно-коммуникационный фактор превратился в одну из важнейших движущих сил современного глобального развития.

«По прогнозам экспертов, объемы информации будут удваиваться каждые два года в течение следующих восьми лет. Один из основных факторов этого роста – увеличение доли автоматически генерируемых данных: с 11% их общего объема в 2005 г. до более чем 40% в 2020-м. При этом используется лишь менее 3% из 23% потенциально полезных данных. К 2020 г. общий объем цифровых

[81] Top 20 Countries with the Highest Number of Internet Users // URL: http://www.internetworldstats.com/top20.htm. (дата обращения: 22.06.2013)

данных достигнет 40 зеттабайт. Для понимания масштаба: если записать 40 зеттабайт данных на самые емкие современные диски Blue-ray, общий вес дисков без упаковки будет равен весу 424 авианосцев»[82].

Мировое информационное пространство тесно связано со всеми сегментами международного сообщества: экономическим, политическим, военным, социальным и др. Все большее влияние на обеспечение национальной и глобальной безопасности оказывают такие процессы, происходящие в мировом сообществе, как:

− глобализация современного мира и происходящих в нем политических процессов;

− информатизация всех основных сфер жизнедеятельности мирового сообщества и индустриально развитых стран;

− переход от индустриальной стадии развития общества к постиндустриальным информационным политическим, экономическим и социальным системам.

1.1. Основные подходы к изучению феномена глобальной безопасности

Проблема поддержания безопасности являлась актуальной на протяжении всей мировой истории. Эта задача является актуальной и в наши дни. В ее решении участвуют отдельные граждане и семьи, социальные группы и нации, государства и союзы государств, международные организации и мировое сообщество.

Для каждого периода мирового развития характерно собственное конкретно-историческое понимание сущности безопасности. Вначале обеспечение безопасности было обусловлено предохранением личности от физического насилия. С появлением государств, их правители и народы считали безопасность обеспеченной, если были приняты соответствующие меры защиты

[82] Сараев В. Когда данные стали большими // Эксперт. 2013. 13–19 мая. № 19. С. 51-54.

от нападения извне. Для поддержания безопасности государства начали заключать военно-политические союзы и создавать военно-политические блоки.

За последние 100–150 лет восприятие безопасности как на государственном, так и на международном уровнях существенно изменилось. Во-первых, значительно увеличилось проблемное поле, которое охватывает категория «безопасность». Данное увеличение произошло, прежде всего, под влиянием глобализации, которая породила огромные миграционные потоки мирового масштаба, глобальный экологический кризис, распространение оружия массового уничтожения, создание мировой экономики и финансовой системы и как следствие, возникновение мировых финансово-экономических кризисов.

Во-вторых, очевидными стали существенные сдвиги в системе приоритетов процесса поддержания безопасности. Эти изменения обусловлены трансформацией принципов и норм, определяющих государственный суверенитет. Существенный вклад в формирование современного состояния безопасности внесло развитие средств информации и связи.

Современная политическая наука рассматривает безопасность в контексте деятельности по выявлению и изучению, а также предупреждению и устранению факторов и условий, которые порождают угрозы и опасности для существования людей. В данной связи В. М. Кулагин пишет: «В самом широком смысле, безопасность – это состояние защищенности от угроз ключевым ценностям. Нередко при определении безопасности акцент делается именно на защищенности – наличии средств и организационных мер, институтов, договоренностей с партнерами и так далее. Но весь комплекс обеспечения защищенности определяется характером и масштабом угроз. Поэтому понятие «безопасность» объединяет неразлучную пару «угрозы – защита от них».[83]

Состояние защищенности от угроз поддерживается на различных уровнях: локальном и национальном, региональном и глобальном. Эти угрозы могут быть достаточно разнообразными и направлены, в первую очередь, против жизненно

[83] Кулагин В. М. Международная безопасность. М.: Аспект Пресс, 2007. С. 8.

важных ценностей, имеющих материальный, духовный и геополитический характеры.

Реализация этих угроз, если не будут приняты соответствующие меры для их ликвидации, в состоянии нанести недопустимый ущерб населению конкретного государства или международного региона. В случае всемирного масштаба угрозы, возможно возникновение ситуации, которая приведет к глобальной катастрофе, если данная опасность не будет устранена.

Таким образом, безопасность в современном мире приобрела принципиально новые характеристики. Страны и народы включаются в мировые процессы, затрагивающие все основные сферы жизнедеятельности человечества. Эти процессы ускоряет колоссальный научно-технический прогресс.

Современный этап мирового развития сопровождается возникновением и обострением политических, экономических, экологических, энергетических и других проблем, получивших глобальный масштаб распространения. Возрастание взаимозависимости государств и регионов мира, создание мировых рынков и региональных общих экономических пространств, появление оружия массового уничтожения, способного истребить все живое на планете, и другие подобные явления в современных условиях выдвинули на первый план проблему обеспечения безопасности в масштабах всего мирового сообщества – то есть проблему обеспечения международной безопасности.

Этот вид безопасности представляет собой такое состояние отношений в мировом сообществе, при котором обеспечиваются стабильность развития мирового и региональных сообществ, защищенность от внешних угроз, право на свободное развитие всех народов, гарантия суверенитета и независимости всех официально признанных государств.

В российской политической науке одно из наиболее полных и развернутых определений международной безопасности предложил А. Г. Арбатов: «Состояние международных отношений, обеспечивающее защищенность государства и легитимность международных организаций и негосударственных субъектов отношений от внешних и трансграничных угроз, позволяющее обеспечить

суверенитет, территориальную целостность, устойчивое развитие и взаимовыгодное сотрудничество государств, эффективное функционирование международных организаций и негосударственных субъектов, а также справедливое мирное урегулирование их конфликтов и согласование экономических, политических, военных и иных интересов»[84].

Международная безопасность обеспечивается с помощью политических и правовых, экономических и военных, а также других способов. В «Стратегии национальной безопасности Российской Федерации до 2020 года» написано: «В сфере международной безопасности Россия сохранит приверженность использованию политических, правовых, внешнеэкономических, военных и иных инструментов защиты государственного суверенитета и национальных интересов. Проведение предсказуемой и открытой внешней политики неразрывно связано с реализацией задач устойчивого развития России»[85].

Большое значение для поддержания такой безопасности имеют демилитаризация, демократизация и гуманизация международных политических процессов, обеспечение социальной справедливости и равенства в международном сообществе, верховенство права в отношениях на мировой арене.

На основе геополитического подхода выделяют следующие измерения международной безопасности: человеческое (личностное), национальное, региональное и глобальное. Данный подход показывает, что международная безопасность непосредственно связана и может оказывать влияние на все субъекты современных международных отношений: от отдельных индивидов до глобальных акторов. Самым непосредственным образом международная безопасность касается всех государств современного мира, как основных субъектов международных отношений, действующих в условиях глобального мира.

---

[84] Арбатов А. Г. Международная безопасность в эпоху перемен и внешняя политика России // Россия в глобальном мире: 2000–2001. Хрестоматия в 6 тт. / Рос. Совет по межд. делам / Под общ ред. И.С. Иванова. М.: Аспект Пресс, 2012. Т. 2. С. 12.

[85] Стратегия национальной безопасности Российской Федерации до 2020 г. Утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537 // Российская газета. 2009. 19 мая. Гл. 4. Ст. 45–46.

Глобальное измерение безопасности наиболее интенсивно расширяется в последнее время, охватывая новые субъекты международных отношений и включая новые сферы жизнедеятельности мирового сообщества, в том числе и глобальное информационное пространство.

Рассмотрим более подробно каждое из выделенных измерений международной безопасности. Человеческое или личностное измерение безопасности связано с созданием и поддержанием нормальных условий жизнедеятельности как для отдельных индивидов, так и для конкретных социальных групп.

Такая деятельность в сфере человеческой безопасности связана как с кризисными экстремальными ситуациями, так и с периодами устойчивого развития общества. Во время кризисов обеспечение безопасности заключается в существовании такой системы мер защиты от угроз, которая позволила бы уберечь людей от гибели вследствие войн, экологических катастроф и преступного насилия, а также от голода и болезней.

В условиях мирного общественного развития речь в рассматриваемом нами случае идет о формировании условий для реализации личностных и социальных интересов. Так, в «Стратегии национальной безопасности Российской Федерации до 2020 года» отмечается: «Стратегическими целями обеспечения национальной безопасности в области повышения качества жизни российских граждан являются снижение уровня социального и имущественного неравенства населения, стабилизация его численности в среднесрочной перспективе, а в долгосрочной перспективе – коренное улучшение демографической ситуации. Повышение качества жизни российских граждан гарантируется путем обеспечения личной безопасности, а также доступности комфортного жилья, высококачественных и безопасных товаров и услуг, достойной оплаты активной трудовой деятельности»[86].

[86] Стратегия национальной безопасности Российской Федерации до 2020 г. Утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537 // Российская газета. 2009. 19 мая. Гл. 2. Ст. 19.

Категория «человеческая безопасность» была сформулирована в 1990-е годы в дополнение к понятию «гражданская безопасность». Детальное раскрытие содержания этого термина дано в «Докладе о человеческом развитии», подготовленном в 1994 г. Программой развития ООН[87]. Это понятие получило широкое распространение. Подобная концепция позволила рассматривать в комплексе проблемы обеспечения безопасности, возникающие как во внутреннем развитии государств, так и на международном уровне.

Если понятие «человеческая безопасность» вошло в общественную практику и политическую науку в конце XX века, то категория «национальная безопасность» появилась в самом его начале. Эта категория была введена в политический дискурс в 1904 году Теодором Рузвельтом – 26-м Президентом США. Он использовал термин «национальная безопасность» для обоснования присоединения зоны Панамского канала, обращаясь с традиционным посланием к американскому Конгрессу.

В дальнейшем понятие «национальная безопасность» получило широкое распространение среди мировой политической элиты и в международном академическом сообществе. В российской политической практике и науке это понятие вошло в обиход в конце 1980-х гг. – когда оно заменило термин «государственная безопасность».

В современной политической науке национальная безопасность трактуется прежде всего, как такое внутреннее состояние и международное положение страны, при котором отсутствует угроза возникновения войны и посягательств на ее суверенитет, независимость и территориальную целостность.

Среди основополагающих документов, определяющих внешнюю политику Российской Федерации, дефиниция национальной безопасности дана в «Стратегии национальной безопасности Российской Федерации до 2020 года». В Стратегии написано: «Национальная безопасность» – состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и

[87] Human Developement Report. UNDP. N. Y.: Oxford University Press, 1994.

уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства»[88]. Этот вид безопасности, безусловно, имеет существенное международное измерение. Так, важным показателем обеспеченности национальной безопасности является отсутствие возможностей для внешнего вмешательства в его дела и, тем более, совершения военного вторжения.

Вторжение США и Великобритании в Ирак (2003 г.) повлияли на осмысление национальной безопасности в мировом сообществе. Стало очевидным, что международно-правовые методы не всегда позволяют обеспечить национальную безопасность суверенного государства и предотвратить военное вмешательство извне.

В связи с этим, в мировом сообществе возникла точка зрения, согласно которой, при несовершенстве международно-правовых способов обеспечения национальной безопасности следует полагаться на силовые методы. В качестве такого силового фактора в первую очередь рассматривается оружие массового поражения (ОМУ), в том числе и ядерное. Одни государства – такие, как КНДР и Ирак – стремятся заполучить это мощнейшее оружие, другие – Индия и Пакистан, уже создавшие ядерные потенциалы, не спешат от них отказываться.

Так, в плане рассматриваемого вопроса полезно мнение, высказанное заместителем Председателя Правительства Российской Федерации Д. О. Рогозиным: «Возьмем в качестве примера ситуацию в Ираке. Мы пока не получили должных объяснений от американской стороны, что они на самом деле думают по поводу истинных причин применения военной силы против Ирака. Внешний повод хорошо известен: якобы наличие у Саддама Хусейна оружия массового уничтожения.

Судя по всему, наши американские коллеги точно знали, что нет там никакого оружия массового уничтожения. Если бы оно было, сложно себе представить, что американцы начали наземную операцию для свержения режима

[88] Стратегия национальной безопасности Российской Федерации до 2020 г. Утверждена Указом Президента Российской Федерации от 12 мая 2009 года. № 537 // Российская газета. 2009. 19 мая. Гл. 1. Ст. 6.

Саддама Хусейна. Для них было бы опасно развязывать такую операцию. Поэтому другие страны сегодня ссылаются именно на этот факт, объясняя свое стремление обладать оружием массового уничтожения. Ведь в таком случае против них точно не будет применяться наземная операция»[89].

Руководство Соединенных Штатов придает большое значение не только мнимой (как в случае с Ираном), но и реальной борьбе с распространением ОМУ, считая ее первостепенной задачей в обеспечении национальной безопасности.

Так, в Стратегии национальной безопасности, выпущенной администрацией Б. Обамы в мае 2010 года, в качестве неотложных задач во внешней политике, требующих решения для обеспечения национальной безопасности США, на первое место поставлена борьба с распространением ОМУ и международным терроризмом. За ними следуют преодоление экономической рецессии и мирового финансово-экономического кризиса, а также продвижение универсальных ценностей за рубежом[90].

Таким образом, можно видеть, что современное понимание национальной безопасности в Соединенных Штатах также имеет явно выраженное международное измерение и затрагивает наиболее болезненные проблемы мирового развития. Следовательно, можно сделать вывод о том, что эффективность обеспечения национальной безопасности современного государства неразрывно связана с особенностями проведения его внешней политики.

Данная политика направлена на осуществление взаимодействия конкретного государства с другими субъектами международных отношений. К таким субъектам принято относить другие государства, объединения и союзы государств, международные организации, а также неправительственные организации и заинтересованные группы.

Внешняя политика связана с обеспечением национальной безопасности в значительной мере благодаря защите национальных интересов страны. Так, под

---

[89] Материалы международной конференции «Ядерное оружие и международная безопасность в XXI в.» / Гл. ред. И. С. Иванов. М.: Спецкнига, 2013. С. 16.

[90] National Secutity Strategy. May 2010. P. 4–5 // http: // nssarchive.us/NSSR/2010.pdf. (дата обращения: 26.10.2013)

национальными интересами Российской Федерации понимают «совокупность внутренних и внешних потребностей государства в обеспечении защищенности и устойчивого развития личности, общества и государства»[91].

В современном глобальном мире защиту своих национальных интересов Россия стремится осуществлять посредством проведения рациональной и прагматичной внешней политики, опирающейся на лучшие исторические традиции российской дипломатии.

При этом, большое значение придается Организации Объединенных Наций как центральному звену стабильной системы международных отношений, а также многосторонним форматам межгосударственного сотрудничества таким, как «Группа двадцати», РИК, БРИКС и др. В основе российской внешней политики лежат такие принципы, как уважение, равноправие и взаимовыгодное сотрудничество государств.

Однако, в современном глобальном мире проведение традиционной внешней политики для успешного отстаивания национальных интересов и обеспечения национальной безопасности на сегодняшний день явно недостаточно. На это обращает внимание Президент Российского совета по международным делам (РСМД) И. С. Иванов: «На протяжении ближайших лет российская внешняя политика, как и наша экономика, должна стать «умной».

Это не означает, конечно, что раньше она была неумной: просто раньше мы использовали (и подчас весьма эффективно!) то, что было под рукой и то, что мы унаследовали от прошлого – в частности, сохранившийся военно-технический потенциал и имеющиеся энергетические ресурсы. В современном мире этого недостаточно, для того чтобы сохранить международные позиции России, тем более – чтобы укрепить их»[92].

Итак, ведущие российские эксперты ставят вопрос о том, чтобы упрочить позиции нашей страны в глобальном мире XXI века и надежно обеспечить ее

---

[91] Стратегия национальной безопасности Российской Федерации до 2020 год. Утверждена Указом Президента Российской Федерации от 12 мая 2009 года. № 537 // Российская газета. 2009. 19 мая. Гл. 1. Ст. 6.

[92] Иванов И. С. Будущее – за «умной» внешней политикой // Россия в глобальном мире: 2000–2011. Хрестоматия в 6 тт. / Рос. Совет по межд. делам / под общ ред. И. С. Иванова. М.: Аспект Пресс, 2012. Т. 1. С. 24.

национальную безопасность недостаточно опираться только на сформировавшиеся исторические традиции российской дипломатии, но и также совершенствовать механизм формирования и реализации внешнеполитических решений. Необходимо поставить и решить принципиально иную задачу – обновить и расширить весь арсенал внешнеполитических инструментов, который потребуется нашей стране в грядущих международных отношениях.

«Умная» внешняя политика, – продолжает И. С. Иванов, – предполагает способность политического руководства воспользоваться максимально широким набором активов, которыми располагают данная страна и данное общество. Включая, конечно, и нематериальные активы, которые часто игнорировались или, как минимум, серьезно недооценивались традиционной дипломатией прошлого.

…Мы пока еще не очень хорошо понимаем и, тем более, не способны контролировать ведущие тенденции мировой политики XXI в. – такие, как повсеместное распространение новых информационно-коммуникационных технологий…»[93].

Традиционно с древнейших времен военная безопасность, обеспечение которой ассоциируется с защищенностью государства от вооруженной агрессии из-за рубежа, рассматривается как центральный элемент системы поддержания национальной безопасности. В XXI веке он также играет важную роль как на национальном, так и на глобальном уровнях международных процессов в сфере безопасности. При этом важное значение имеет состояние вооруженных сил конкретной страны.

В настоящее время арсеналы ведущих держав пополняются оружием, созданным на основе инновационных подходов. К таким видам новейших вооружений следует отнести ядерные заряды малой мощности, стратегические ракеты с неядерными боеголовками, высокоточное оружие, беспилотные летательные аппараты и тому подобное. Гонка вооружений вышла в космическое пространство, а ее бесспорным лидером являются Соединенные Штаты, военный бюджет которых составляет почти половину всех мировых расходов на оборону.

[93] Там же. С. 25.

С. В. Кортунов, анализируя состояние военной безопасности в современном глобальном мире, подчеркивает, что: «…ведущие страны не только не расстаются с арсеналами, явно превышающими уровень необходимой обороны, но и, наоборот, постоянно совершенствуют их, включая наступательные виды вооружений. Использование дипломатических методов, строгое соблюдение общепризнанных принципов и норм международного права так и не стали доминирующей тенденцией при решении проблем международной безопасности»[94].

«Региональная безопасность» представляет собой еще одно значимое измерение безопасности в современном глобальном мире. Ее следует рассматривать как важное звено системы международной безопасности. Она является производной от текущей ситуации в сфере международных отношений определенного региона, входящего в состав мирового геополитического пространства. Обеспечение этой безопасности означает, что регион свободен от военных угроз, экономических кризисов, гуманитарных и экологических катастроф и тому подобное.

В наши дни трудно полностью отделить региональную безопасность от национальной и глобальной. Создавая систему безопасности в регионе, входящие в него государства опираются на национальные системы в рассматриваемой сфере. Определенные структуры из национальных систем могут входить, в качестве составных частей или элементов, в систему безопасности большего – регионального масштаба и наоборот, региональные институты и организации могут решать задачи обеспечения безопасности на региональном уровне.

При соотнесении регионального и глобального уровней безопасности становится очевидным, что обеспечение безопасности в ряде регионов мирового сообщества осуществляется разными путями. Это зависит в первую очередь от того, какие формы в регионе приобретают те или иные процессы региональной интеграции. В конце прошлого века получала распространение концепция открытого регионализма, которая в начале применялась для изучения

[94] Кортунов С. В. Мировая военно-политическая ситуация. Год 2025 // Международная жизнь. 2010. № 3. С. 27.

региональной экономической интеграции и ее взаимосвязи с глобальными экономическими процессами. Эксперты отмечают, что «концепция «открытый регионализм» представляет собой такую модель организации торгово-финансовых отношений, которая сочетала бы в себе как соблюдение глобальных соглашений, так и поощрение практики договоренностей, достигнутых на региональном уровне. При этом экономическая заинтересованность способствует политическому сотрудничеству посредством упрощения процедур, связанных с пересечением политико-правовых пространств»[95].

Таким образом, открытый регионализм характеризует первый путь регионального развития, когда интеграционные процессы на уровне региона тесно связаны с процессом глобализации. Второй путь – «закрытый регионализм» – является полной противоположностью рассмотренному ранее открытому регионализму, так как ориентирован на создание в регионе обособленного, или замкнутого, объединения государств, ориентированных, главным образом, на внутренние ресурсы в региональном развитии.

Данный подход в условиях современного глобального мира можно применить к процессам обеспечения региональной безопасности, хотя границы между открытым и закрытым регионализмом в сфере безопасности провести сложнее, чем в экономической области.

С одной стороны, сотрудничество в сфере безопасности, как правило, носит закрытый характер в силу специфики и особенностей ее обеспечения. Не являются исключением из этого правила и институты региональной безопасности. Даже, когда деятельность таких институтов носит публичный и открытый характер, они все-таки ориентируются на региональные интересы, на сохранение региональной идентичности, как одного из условий обеспечения безопасности.

В то же время, в современном глобальном мире в условиях возрастания взаимозависимости всех основных субъектов международных отношений, замкнутые региональные группировки не всегда могут эффективно действовать, в том числе и в сфере обеспечения безопасности. Внешнеполитические интересы

[95] Косов Ю. В., Фокина В. В. Политическая регионалистика. СПб.: Питер, 2009. С. 65.

государств – участников международных организаций, действующих в области региональной безопасности, подталкивают данные институты к выходу за пределы своего региона и даже к участию в процессах, связанных со сферой глобальной безопасности.

Интересное наблюдение при изучении рассматриваемой проблемы сделала Т. В. Юрьева: «Специфической формой открытого регионализма становится формирование своего рода рынка услуг безопасности. Региональные структуры безопасности – в первую очередь европейские – становятся поставщиками такого рода услуг в глобальном масштабе. Прежде всего, это касается сферы регулирования конфликтов. Организация Северо-Атлантического договора (НАТО), следом за ней – Европейский Союз и Организация Договора о коллективной безопасности (ОДКБ) на рубеже XX и XXI вв. начинают участвовать (либо готовятся к участию) в регулировании конфликтов за пределами своего региона. Отсюда – появление на этом рынке отношений конкуренции/кооперации и поиск механизмов регулирования этого глобализирующегося рынка»[96].

На региональные процессы в сфере безопасности оказывают влияние геополитические факторы, связанные с изменением региональных границ и процессами субрегионализации. Особенно наглядно данные процессы проявляются на Европейском континенте. Как геополитическое понятие, Европа не поддается однозначному определению. Во второй половине XX века сформировались несколько концепций геополитической конфигурации Европы.

Первая концепция – «Европа от Польши до Португалии» (или, в другом варианте, «от Бреста до Бреста») в годы «холодной войны» исключала из европейского пространства две сверхдержавы, США и СССР, а теперь его правопреемницу – Россию. Однако, уязвимое место рассматриваемой концепции в том, что она не учитывает ту роль, которую играют США и Россия в европейской политике. При игнорировании влияния этих держав многие явления

[96] Юрьева Т. В. Проблемы региональной безопасности: современный опыт Европы // Вестник МГИМО-Университета. 2010. № 6. С. 127.

и процессы в европейском развитии оказываются трудно объяснимыми или не поддающимися пониманию вообще.

Вторая концепция получила название «Европа от Атлантики до Урала», и была выдвинута президентом Французской Республики Шарлем де Голлем. Подобная трактовка пользовалась поддержкой советского руководства. Это было связано с тем, что она включала в европейское геополитическое поле СССР, хотя и в усеченном виде (только от западной границы до Урала) и оставляла за его пределами североамериканские государства (США и Канаду). Данная концепция существенного значения для международных отношений в Европе не имела из-за явного игнорирования, как и предыдущей теорией, очевидных геополитических реалий.

Третья концепция, которую принято именовать «Хельсинкская Европа» («от Ванкувера до Владивостока»), прагматично и гибко отразила политико-силовые и геостратегические реальности послевоенной ситуации на Европейском континенте. Именно в Хельсинки состоялись основные этапы (первый и третий) Совещания по безопасности и сотрудничеству в Европе. Здесь в 1975 году была подписана Хельсинкская декларация. Рассматриваемая концепция способствовала определенной разрядке напряженности в Европе, наведению мостов между Западом и Востоком.

Однако, со временем проявилась и ограниченность такого подхода. Главный недостаток концепции – отсутствие в ней четко определенных геополитических границ Европы. В результате к европейскому геополитическому пространству оказались отнесенными государства, которые, во-первых, значительно удаленные географически от рассматриваемой части света, во-вторых, принадлежащие к другой цивилизации и имеющие иную, неевропейскую культуру[97].

В настоящее время внутри европейского геополитического пространства идут процессы субрегионализации. Наблюдается явно выраженный процесс

[97] Подробнее см.: Косов Ю.В. Мировая политика и международные отношения // Политология. Под ред. М. А. Василика. М.: Гардарика, 2008. С. 534–537.

формирования двух наиболее крупных субрегионов Европейского континента. Один из них формируется вокруг Северо-Алантического альянса (НАТО) и Европейского союза; другой – в рамках Содружества Независимых Государств и Организации договора коллективной безопасности, а в перспективе и Евразийского союза. Кроме того, в последние два десятилетия в Европе начались процессы формирования субрегионов, локализация которых не совпадает с пределами геополитических пространств, входящих в зоны контроля вышеуказанных международных организаций. В качестве таких новых геополитических субрегионов следует назвать Балтийский, Черноморско-Каспийский, Кавказский субрегионы, а также субрегион Юго-Восточной Европы.

«Для определения факторов структуризации европейского региона безопасности, – отмечает Т. В. Юрьева, – теоретически по-прежнему применимы как реалистическая, так и либеральная парадигмы: соответственно – по общности интересов безопасности и – по общности базовых общественных ценностей. Возможен синтез этих двух парадигм, если под региональным интересом безопасности понимать региональный консенсус по общеевропейским ценностям. В любом случае, в нынешнем столетии Европе «от Ванкувера до Владивостока» нужны иные геополитические скрепы для сохранения единого пространства на паневропейском уровне, отличные от тех, которые существовали во времена холодной войны»[98].

Глобальная безопасность связана с обеспечением защиты мирового сообщества от угроз планетарного масштаба. Данные угрозы бросают реальные вызовы всему человечеству. Если на эти вызовы не находить адекватные и своевременные ответы, то могут возникнуть сначала потенциальные, а затем – и реальные опасности существованию людского рода или сложатся условия для резкого ухудшения условий жизнедеятельности во всем глобальном мире. Под данными вызовами, как правило, понимают глобальные проблемы мирового развития.

Таким образом, поддержание глобальной безопасности неразрывно связано

[98] Юрьева Т. В. Указ соч. С. 130.

с поисками путей решения или с ослаблением давления глобальных проблем на человечество. Под этими проблемами понимают явления планетарного характера, которые, в той или в иной степени, оказывают влияние на жизнедеятельность человечества в целом, всех государств и народов, каждого жителя планеты. Глобальные проблемы следует рассматривать как реальный фактор современного мирового развития.

Термин «глобальные проблемы» получил широкое распространение сначала в академическом сообществе, а затем – и в политических кругах во второй половине прошлого века. В процессе изучения и осмысления феномена глобальных проблем была введена в научный и политический лексиконы категория политической науки – «глобальная безопасность» (в ее современном значении).

Глобальная проблематика представляет собой комплексную иерархическую систему, в ходе развития которой происходят достаточно динамичные изменения. В различные исторические периоды центральное место в процессах обеспечения глобальной безопасности занимали различные планетарные проблемы. В годы «холодной войны» это была проблема предотвращения мировой ядерной войны, затем внимание было сосредоточено на преодолении глобального экологического кризиса, в самом начале XXI века на первый план выдвинулась угроза международного терроризма и так далее. И в наши дни в фокусе внимания ученых-глобалистов находятся вопросы, связанные с определением актуальности конкретных глобальных проблем и их иерархии в целом.

При изучении данного феномена весьма полезной является точка зрения В. Г. Барановского. Российский исследователь приходит, в частности, к следующему выводу: «Наиболее важными направлениями действий в сфере глобальных проблем в настоящее время являются:

− преодоление бедности, борьба с голодом, содействие социально-экономическому развитию наиболее отсталых стран и народов;

− поддержание экологического и климатического баланса, минимизация негативных воздействий на среду обитания человечества и биосферу в целом;

− решение крупнейших глобальных проблем в области экономики, науки, культуры, здравоохранения;

− предупреждение и минимизация последствий природных и техногенных катастроф, организация спасательных операций (в том числе по гуманитарным мотивам);

− борьба с терроризмом, международной преступностью и другими проявлениями деструктивной активности;

− организация порядка на территориях, утративших политико-административную управляемость и оказавшихся во власти анархии, угрожающей международному миру»[99].

Обеспечение глобальной безопасности в современном мире представляет собой процесс, который имеет всеобщий характер и всеобъемлющее измерение. Под всеобщим характером понимают то, что для поддержания данного вида безопасности необходимы скоординированные действия всех субъектов международных отношений.

Всеобъемлющее измерение безопасности на глобальном уровне обусловлено необходимостью учета при ее обеспечении всех кризообразующих факторов и проблемных зон глобального развития и принятия мер для поддержания состояния устойчивости всех основных жизнеобеспечивающих систем мирового сообщества.

Всеобщий и всеобъемлющий характер в современном мире имеет также процесс информатизации. Этот процесс является и глобальным процессом, а еще ему присущ общецивилизационный характер. Информатизация является важнейшей и долговременной тенденцией развития мирового сообщества. Она находится в тесной взаимосвязи с другим подобным процессом всемирного масштаба – глобализацией.

Во-первых, многие проявления глобализации в формировании и развитии мировой экономики, финансов, энергетики, а также институтов глобального управления оказались бы невозможными без возникновения и широкого

[99] Барановский В. Г. Трансформация мировой системы в 2000-х гг. // Международные процессы. 2010. Т. 8. № 1.

распространения информационно-коммуникационных технологий.

Во-вторых, само распространение информационно-коммуникационных технологий в таких масштабах, какие оно приняло в наши дни, является результатом деятельности транс- и многонациональных компаний, а также глобализации экономической и всех других основных сфер жизнедеятельности человечества.

«Глобальная информатизация общества открывает не только новые возможности для развития человека и социума, – отмечает К. К. Колин, – но и способствует возникновению новых угроз на этом пути. В первую очередь, речь идет о комплексе проблем информационной безопасности (в их числе наиболее значимыми являются виртуализация общества и использование новых технологий для манипуляции общественным сознанием), а также противоборство в информационной сфере, которое в последние годы становится глобальным, все заметнее принимая характер информационных войн»[100].

1.2. Трансформация политики безопасности в условиях изменения статуса России в современном международном сообществе

На протяжении всей мировой истории между ведущими государствами идет постоянное соревнование, а в определенные исторические периоды и борьба, включая ее вооруженные формы: конфликты и войны за влияние в международном сообществе. Президент Российской Федерации В. В. Путин в Послании Федеральному Собранию 12 декабря 2012 года подчеркнул: «В мире XXI века, на фоне новой расстановки экономических, цивилизационных, военных сил, Россия должна быть суверенной и влиятельной страной. Мы должны не

[100] Глобальные процессы, безопасность и устойчивое развитие. Материалы «круглого стола» // Alma Mater. 2012. Март. № 3. С. 12.

просто уверенно развиваться, но и сохранить свою национальную и духовную идентичность, не растерять себя как нация. Быть и оставаться Россией»[101].

Как показывает опыт предыдущих столетий развития международного сообщества, входившие в него страны весьма неравномерно приобретали, усиливали и утрачивали свое влияние. Известны времена господства Испании, Франции, Англии и других держав. В XIX веке в дипломатических и политических кругах Европы начали использовать понятие «великая держава».

История возникновения этого понятия восходит к Венскому конгрессу (1814–1815 гг.), на котором был учрежден новый международный порядок. Этот порядок, как известно, основывался на балансе сил основных держав и на их политике, направленной на мирное разрешение противоречий между собой, получившей название «европейский концерт».

«Те страны, на которые опирался новый порядок и от которых зависел «европейский концерт», со времени Венского конгресса получили неофициальное название великих держав»[102]. Первоначально к числу великих держав относили Австрию, Великобританию, Пруссию и Россию, но вскоре к ним присоединилась Франция. В число великих держав во второй половине XIX века вошло еще одно европейское государство – Италия (после того как закончилось объединение этой страны).

Вслед за представителями Южной Европы в круг наиболее влиятельных участников международных отношений вошли и государства, не принадлежащие к Европейскому континенту: ими стали США и Япония.

Первая и Вторая Мировые войны существенно изменили геополитический баланс в мире. Это сказалось и на составе клуба мировых держав. К этому клубу стали относить постоянных членов Совета Безопасности Организации Объединенных Наций (СБ ООН провел первое свое заседание в январе 1945 года). Ими стали державы – победители во Второй Мировой войне, составившие основу

---

[101] Путин В. В. Послание Президента Федеральному Собранию. 12 декабря 2012 г. // http://президент.рф/news/17118 (дата обращения: 23.10.2013)

[102] История международных отношений. В 3 тт. / Под ред. А. В. Торкунова, М. М. Наринского. – М.: Аспект Пресс, 2012. Т. 1. С. 193–194.

антигитлеровской коалиции: СССР, США, Великобритания, Китай и Франция. В Совете Безопасности ООН действует принцип единогласия постоянных членов. Этот принцип означает, что в случае, когда хотя бы один из постоянных членов при обсуждении любого вопроса проголосовал «против», то решение не может быть принято. Таким образом, великие державы – постоянные члены СБ ООН – обладают «правом вето» (это латинское слово переводится на русский язык как «запрещаю») при решении важнейших вопросов мировой политики, связанных с обеспечением безопасности в мире.

Принятие принципа единогласия было связано с тем, что, создавая ООН, великие державы – победители во Второй Мировой войне строили планы сохранить единство в борьбе с возможными агрессорами и после ее окончания. «Холодная война» эти планы разрушила, однако, и в самые трудные годы этого исторического периода Совбез ООН оставался политическим органом, в рамках которого великие державы постоянно взаимодействовали друг с другом.

В настоящее время ООН продолжает играть центральную роль в системе международных отношений, обладая уникальной легитимностью. Однако, в международном сообществе утвердилась точка зрения о необходимости реформы Организации Объединенных Наций и некоторых ее главных органов, включая Совет Безопасности.

Причин для этого накопилось немало. Поводов для проведения реформы, по мнению экспертов-международников, более чем достаточно. Среди них наиболее часто упоминают: трансформацию всей глобальной системы международных отношений за более чем 60 лет, прошедших с момента создания ООН, значительное изменение баланса сил среди наиболее развитых и влиятельных государств, изменение роли целых регионов в мировых политических процессах, возникновение и обострение глобальных проблем.

Постоянный представитель Российской Федерации при ООН и Представитель Российской Федерации в Совете Безопасности ООН В. И. Чуркин, обсуждая данный вопрос, высказывает следующую точку зрения: «В том, что касается реформы Совета Безопасности – самой «горячей» темы реформенной

повестки, – то в этой сфере говорить об обозначении контуров согласия еще рано. Сближение подходов государств-членов пока не просматривается. Цель этой реформы мы также видим в том, чтобы в результате возросла практическая отдача от работы Совета Безопасности, оперативность принятия им решений. Разумеется, при всех вариантах расширения состава Совета, статус нынешних постоянных членов СБ, включая право вето, должен оставаться неизменным»[103].

Наиболее вероятными претендентами на вхождение в реформированный Совет Безопасности в качестве постоянных членов рассматриваются Япония, Германия, Индия и Бразилия.

Итак, исходя из приведенного выше краткого исторического анализа, можно сделать вывод о том, что со времени появления в международном сообществе клуба великих держав, вплоть до сегодняшнего дня, Россия входит в его состав. В то же время, как показывает исторический опыт, статус великой державы нельзя продлевать автоматически. Право называться великой державой страна должна постоянно подтверждать, играя ведущую роль в мировом развитии, в том числе и в процессе поддержания глобальной безопасности.

С начала XXI века международный статус нашей страны и ее роль в мировых делах, в определенной мере снизившиеся после распада СССР, вновь стали возрастать. Россию, как и раньше, все основные субъекты международных отношений признают в качестве великой мировой державы. Об этом свидетельствует участие Российской Федерации в ведущих международных организациях. Уже говорилось о том, какое важное место занимает наша страна в ООН, являясь постоянным членом Совета Безопасности и государством – учредителем этой организации.

Важным событием в мировой экономике стало образование и деятельность «Группы двадцати» наиболее индустриально развитых стран. В составе этого неформального международного института Россия сотрудничает с ведущими государствами современного мира по многим направлениям, участвует в

[103] Чуркин В. И. ООН – непревзойденный игрок на мировом поле // Международная жизнь. 2010. № 9. С. 78 .

обсуждении и поиске путей решения многих мировых финансово-экономических проблем.

Важное место среди них занимают проблемы обеспечения международной экономической безопасности. В 2013 году Российская Федерация председательствовала в данном элитном клубе лидеров глобальной экономики.

Статус России как великой державы подкрепляет ее участие в создании ряда современных международных организаций, в которых наша страна играет ведущую роль. В первую очередь, рассматривая данные международные институты, следует отметить Содружество Независимых Государств (СНГ), Евразийское экономическое сообщество (ЕврАзЭС), Организацию договора коллективной безопасности (ОДКБ), и Шанхайскую организацию сотрудничества (ШОС).

Например, ОДКБ была учреждена в 2002 году. В эту организацию входят семь постсоветских государств: Россия, Армения, Белоруссия, Казахстан[104], Киргизия, Узбекистан и Таджикистан. ОДКБ решает задачи по обеспечению безопасности воздушных границ, предупреждению угроз терроризма и борьбы с незаконным оборотом наркотиков[105].

В конце 2003 года рассматриваемая организация получила статус наблюдателя при ООН. Данный статус означает, что ОДКБ является полноценной международной организацией и, в соответствии с главой 8 Устава ООН, признана в качестве регионального объединения по безопасности[106].

В своей деятельности обсуждаемый международный институт уделяет все возрастающее внимание вопросам обеспечения информационной безопасности. «Мы считаем, что сегодня вопросы информационной деятельности в сфере безопасности, – подчеркивает Генеральный секретарь ОДКБ Н. Н. Бордюжа, – это вопрос номер один. Не нужно никаких войск, не нужно спецподразделений, не нужно огромного количества оружия для того, чтобы дестабилизировать обстановку в каком-нибудь государстве. Можно просто нацелить на него свои

[104] Об информатизации: Закон Республики Казахстан от 11.01.2007 г. № 217-III.
[105] О защите информации: Закон Республики Таджикистан от 02.12.2002 г. № 71.
[106] О свободе информации: Закон Республики Армения от 23.09.2003 г. № 3Р-11.

информационные ресурсы и работать в соответствии с уже существующими технологиями, потихоньку раскачивая там ситуацию посредством воздействия на общественное мнение»[107].

Другой пример – БРИКС: быстро набирающий влияние в мире международный неформальный институт, объединяющий пять восходящих государств-гигантов (Бразилию, Россию, Индию, Китай и Южную Африку). На страны БРИКС приходится свыше 40% населения планеты, более 29% земной суши без Антарктиды, четверть мирового ВВП и так далее.

Как известно, первый саммит БРИКС был проведен по инициативе Президента Российской Федерации В. В. Путина в Екатеринбурге (2009 г.). В наши дни российское руководство данный международный институт признает как фундаментальный фактор современного глобального развития, который будет определять этот процесс в достаточно долгосрочной перспективе.

Согласно оценкам экспертов, влияние БРИКС в международном сообществе будет возрастать как в вопросах мировой политики, так и в такой важнейшей сфере, как мировая экономика и международные финансовые отношения.

В частности, исполнительный директор Национального комитета по исследованию БРИКС Г. Топорая отмечает, что через участие в данном неформальном международном институте Россия намерена «обеспечивать мир и безопасность на основе уважения суверенитета и территориальной целостности других государств, невмешательства в их внутренние дела»[108].

Большую роль в обеспечении глобальной и региональной безопасности играет еще одна международная организация – Шанхайская организация сотрудничества (ШОС). Россия также является активным учредителем ШОС и одним из ее наиболее влиятельных участников.

Эта авторитетная, формально региональная, но имеющая большое влияние на мировую политику организация, объединяющая пять азиатских стран (Китай,

---

[107] Бордюжа Н. Н. Есть вещи, которые для нас запретны // Коммерсантъ. 2013. 26 марта.
[108] Топорая Г. БРИКС: попытка согласования долгосрочной стратегии // http://russiancouncil.ru/inner/?id_4=1506#top. (дата обращения: 15.10.2013)

Казахстан, Узбекистан, Киргизию и Таджикистан) и одно евро-азиатское государство – Россию. Лидеры этой организации – Китай и Россия – занимают ведущие позиции в мировой политике и экономке.

Руководитель Центра стратегических проблем Северо-Восточной Азии и Шанхайской организации сотрудничества при Институте Дальнего Востока РАН С. Г. Лузянин пишет: «В сфере безопасности ключевым для ШОС в ближайшие годы может стать афганский фактор. Требуется обновленная афганская стратегия организации с учетом предстоящих в этой стране изменений – вывода коалиционных сил, возможностей возобновления гражданской войны, создания в республике нового «северного альянса» и так далее.

Специфика позиции ШОС – подготовка к долгосрочным социально-экономическим программам помощи правительству Х. Карзая и акцент на решение соответствующих задач в регионе. Данную программу ШОС целесообразно проводить под эгидой Организации Объединенных Наций»[109].

В мае 2014 года Российская Федерация, Республика Беларусь и Республика Казахстан объявили о создании Евразийского Экономического союза (ЕАЭС).

Таким образом, высокий международный статус России в современном международном сообществе как великой мировой державы подтверждается ее значительной вовлеченностью в процессы глобального развития на самом высоком уровне.

О высоком статусе свидетельствует также участие нашей страны в элитных и наиболее влиятельных международных институтах, а также в организациях глобального и регионального масштаба, в которых она находится на первых ролях. Россия, имея такие уникальные возможности, активно участвует в процессах обеспечения международной безопасности. В последнее время наша страна, в рамках указанной деятельности, все большее внимание уделяет обеспечению глобальной информационной безопасности.

---

[109] Лузянин С. Г. ШОС: проблемы безопасности и перспективы сотрудничества в Евразии // Проблемы Дальнего Востока. 2011. № 1. С. 15.

За последние более чем два десятилетия после окончания «холодной войны» происходит серьезная трансформация политики безопасности в современном мире. Такие изменения были обусловлены трансформацией всей системы международных отношений.

Распад биполярной системы, в которой отношения между великими державами носили конфронтационный характер, открыл дорогу для конструктивного взаимодействия между всеми глобальными игроками на мировой арене, которое было прервано в годы «холодной войны». В результате в политике обеспечения международной безопасности в глобальном масштабе произошли следующие изменения.

Во-первых, были созданы благоприятные перспективы для урегулирования локальных и региональных конфликтов. Появились новые возможности для развития сотрудничества в борьбе с международным терроризмом, религиозным и этническим экстремизмом, а также трансграничной организованной преступностью. Расширилось взаимодействие в обеспечении нераспространения оружия массового уничтожения. Установились более доверительные отношения между ведущими державами в военной сфере.

В этот период получила распространение модель кооперативной безопасности. Например, А. А. Сергунин отмечает, что «модель кооперативной безопасности стала популярной с середины 1990-х гг. «С одной стороны, она признает многомерный характер международной безопасности, а с другой – устанавливает определенную иерархию приоритетов и нацеливает международных акторов на решение первоочередных задач.

…После событий 11 сентября 2001 г., приведших к созданию широкой международной антитеррористической коалиции, мировые внешнеполитические и интеллектуальные элиты стали отдавать предпочтение кооперативной модели»[110].

[110] Сергунин А. А. Международная безопасность: новые подходы и концепты // ПОЛИС. Политические исследования. 2005. № 6. С. 130.

Во-вторых, возникновение условий для широкого международного сотрудничества по обеспечению нераспространения ядерного оружия, критических материалов и технологий. В качестве особо опасной угрозы международной безопасности специалисты рассматривают ситуацию, при которой ядерным оружием или материалами, пригодными для его изготовления, могут завладеть террористические структуры или группы, способные на совершение актов «катастрофического террора».

В-третьих, значительное расширение процесса ограничения и сокращения вооружений, который, однако, приобрел противоречивый характер. К позитивной составляющей этого процесса следует отнести, в первую очередь. принципиальное сокращение ядерных арсеналов в мире. За период, прошедший со времени окончания «холодной войны» они уменьшились примерно в десять раз.

В то же время демонтированной оказалась система ограничения противоракетной обороны после выхода США в 2002 году из Договора ПРО. Кроме того, как известно, Соединенные Штаты, в настоящее время, проводят развертывание глобальной системы ПРО[111].

В-четвертых, продолжают постоянно модернизироваться, а в некоторых регионах мира и увеличиваться арсеналы обычных вооружений. Таким образом, обычные вооружения являются основной материальной базой для локальных и региональных конфликтов, полем для региональных гонок вооружений.

Мировое сообщество стремится взять под некоторый контроль мировую торговлю обычными вооружениями. Генеральная Ассамблея ООН 2 апреля 2013 года приняла Договор о торговле оружием. «За» проголосовали 154 страны, «против» 3, а воздержались 23 государства, в том числе Россия и Китай.

Такая позиция нашей страны обусловлена тем, что Договор не предусматривает конкретные механизмы исполнения и контроля за его

[111] См.: Кучерявый М.М. Космическое измерение военной безопасности Российской Федерации: геополитический анализ // Власть. 2009. № 1. С. 7–12; его же, Потенциальные угрозы безопасности России в воздушно-космическом пространстве // Управленческое консультирование. 2009. № 1; его же, Проблемы обеспечения военной безопасности России в воздушном и космическом пространстве // Личность. Культура. Общество. 2009. №№ 1–2 . С. 323–329.

соблюдением. В связи с этим интересно привести мнение профессора публичного международного права Университета Гринвича Стивена Хайнса: «Правда, не следует ожидать слишком многого от этого документа. Он призван регулировать мировую торговлю оружием, а не создавать всеобщий мир и безопасность. Это было бы неплохо, но одного регулирования торговли оружием здесь будет явно недостаточно. Не думаю, что этому Договору удастся на самом деле предотвратить возникновение конфликтов»[112].

Итак, исходя из вышеизложенного, в общей стратегии укрепления безопасности на обозримый период российские эксперты выделяют четыре основных направления.

Первое направление: сотрудничество великих держав и всех ответственных государств в предотвращении и урегулировании локальных и региональных конфликтов через миротворчество, принуждение к миру и миростроительство в рамках существующих правовых норм и институтов.

Второе направление: взаимодействие в пресечении распространения ядерного оружия и других видов ОМУ и его носителей, опасных технологий и материалов. Укрепление норм Договора о нераспространении ядерного орудия (ДНЯО), режимов экспортного контроля, ужесточения санкций к их нарушителям.

Третье направление: в целях продвижения на первом и втором направлениях – интенсификация переговоров по ограничению и сокращению ядерных вооружений и стратегических средств в неядерном оснащении, придание этому процессу многостороннего формата, контролируемое уничтожение других видов ОМУ, сотрудничество великих держав в создании систем ПРО.

Четвертое направление: в сочетании с представленной выше обширной и взаимосвязанной системой взаимодействия государств в поддержании мира – объединение усилий для решения проблем финансово-экономического

[112] Хайнс С. Договор о торговле оружием: далек от совершенства, но лучше чем ничего. Интервью М. Просвирякова, РСМД // http://russiancouncil.ru/inner/?id_4=1730#top (дата обращения: 07.02.2014)

миропорядка, климата, окружающей среды, дефицита энергоресурсов, продовольствия и пресной воды, демографических потоков и кризисов[113].

Как видно, приведенная выше общая схема стратегии укрепления безопасности ориентирована на деятельность государств и других субъектов, связанных с данной сферой в реальном геополитическом пространстве международных отношений. Однако, с появлением информационных угроз и киберугроз действия по обеспечению информационной безопасности как важного элемента международной безопасности начинают распространяться и на виртуальную сферу: в виде глобального информационного пространства.

Сегодня, благодаря новейшим информационно-коммуникационным технологиям, появились возможности создавать искусственные миры и выдавать их за реальные. Особо значимую роль в создании таких миров играют электронные средства массовой информации и коммуникации: в первую очередь, телевидение, включая глобальные телевизионные сети, и Интернет.

Образ мира и картина процессов обеспечения международной безопасности, как они существуют в реальном геополитическом пространстве, не всегда совпадают с аналогичными образами и картинами в искусственном, виртуальном мире, представляемом в глобальном информационном пространстве.

На возможные последствия такого несовпадения обращает внимание российский исследователь, профессор МГУ А. П. Кочетков: «Новейшие информационно-коммуникационные технологии создают принципиально иное, неведомое ранее «глобальное пространство – время»: локальное, ограниченное пространство буквально становится мировым, а конкретное время приобретает относительный характер, ибо не столько важно то, когда и как именно произошло то или иное событие, сколько то, когда и как оно было представлено и воспринято.[114]

---

[113] См.: Арбатов А.Г. Международная безопасность в эпоху перемен и внешняя политика России // Россия в глобальном мире: 2000–2001. Хрестоматия в 6 тт. / Рос. Совет по межд. делам / под общ ред. И. С. Иванова. М.: Аспект Пресс, 2012. Т. 2. С. 20.

[114] Информационно-коммуникационные технологии, общеорганизационное планирование ресурсов и обеспечение безопасности, послеаварийного восстановления и бесперебойного функционирования систем: Резолюция Генеральной Ассамблеи ООН № A/RES/63/262 от 24 декабря 2008 года [Электронный ресурс]. – Режим доступа:

В этой связи становится очевидным, что даже незначительные, на первый взгляд, изменения в содержании и направленности передаваемого сообщения могут иметь далеко идущие для всего общества последствия, в том числе и в политическом плане»[115].

Таким образом, для современных процессов в сферах национальной и международной безопасности характерны следующие тенденции:

− повышение значимости информации и знаний для обеспечения безопасности как в национальном, так и в глобальном масштабах;

− увеличение доли информационных коммуникаций, средств и продуктов, используемых в процессе обеспечения безопасности;

− зависимость современного прогресса в сфере обеспечения национальной и международной безопасности, прежде всего, от успехов в развитии информационных технологий и связанных с ними областей народного хозяйства.

Итак, уровень развития информационно-коммуникационных технологий в нашей стране сегодня непосредственно связан с ее возможностями в сфере обеспечения собственной безопасности и весьма престижным участием в поддержании международной безопасности. Развитие новых технологий может позволить государству занять более высокое место в ведущих рейтингах стран по уровню развития информатизации или информационно-коммуникационных технологий.

Данные рейтинги начинают оказывать существенное влияние на статус государства в международном сообществе. Однако, дело не только в статусе. Уровень информатизации в наши дни является одним из реальных показателей возможностей страны осуществлять устойчивое внутреннее развитие, успешно защищать внешнеполитические интересы и обеспечивать национальную безопасность в целом.

---

http://daccess-dds-ny.un.org/doc/UNDOC/ GEN/N08/486/53/PDF/N0848653.pdf?OpenElement. (дата обращения: 20.10.2013)

[115] Кочетков А. П. Власть и элиты в глобальном информационном обществе // ПОЛИС. Политические исследования. 2011. № 5. С. 9.

«Телекоммуникации, информационные технологии, цифровые медиа – сфера, которая во всем мире подвержена непрерывным, стремительным, кардинальным изменениям. Ежесекундно во всех странах, в сердце мировых технологических инноваций – Калифорнийской Кремниевой долине, в научно-исследовательских центрах, за стенами корпораций мировых гигантов, ведутся маркетинговые войны за оригинальную идею, прорывное решение, новое предложение, нового покупателя.

Отрасль коммуникаций и новых технологий, проникая во все сферы повседневной деятельности человека, является одной из самых значимых по степени влияния на нашу частную и рабочую жизнь, социальную сферу, экономику, имидж и статус страны в мировом сообществе»[116].

На основании изложенных ранее доводов, можно предположить, что возникновение в мировом сообществе на базе группы передовых индустриально развитых стран сферы высоких информационных технологий представляет собой серьезный глобальный вызов для Российской Федерации. В чем суть этого вызова?

Во-первых, задержка в развитии информационно-коммуникационных технологий, в построении информационного общества, основанного на передовых знаниях, способна привести к серьезному социально-экономическому отставанию от государств – мировых лидеров. Данное отставание может негативно сказаться на внешнеполитическом потенциале страны и ослабить ее позиции как ведущей мировой державы.

Так, Концепцией и Стратегией развития информационного общества в Российской Федерации, утвержденной Президентом Российской Федерации 7 февраля 2008 года № Пр-212 и Государственной программой Российской Федерации «Информационное общество (2011–2020 годы)», утвержденной распоряжением Правительства Российской Федерации от 20 октября 2010 года № 1815-р, определено, что «одним из вызовов, на который должна ответить

[116] Развитие отрасли инфокоммуникационных технологий (ИКТ) в России // CRN ИТ-БИЗНЕС. 2012. 01 августа. // http://www.crn.ru/news/detail_print.php?ID=68520&print=Y. (дата обращения: 29.11.2013)

Российская Федерация, является переход развитых стран к формированию новой технологической базы экономических систем, основанной на использовании новейших достижений в области информатики, в том числе в здравоохранении и других сферах[117].

Ответ на этот вызов – инновационный сценарий, направленный на формирование новой экономики, или экономики знаний и высоких технологий, в число ведущих отраслей которой входят отрасли связи и информационных технологий»[118].

Во-вторых, овладение высокими информационно-коммуникационными технологиями и инновационными подходами для их дальнейшего развития необходимо для обеспечения национальной безопасности нашей страны. В условиях глобального информационного общества происходит трансформация систем международной и национальной безопасности и их обеспечения в современных условиях стало невозможным без подержания на должном уровне их информационной безопасности.

В приведенных выше Стратегии развития информационного общества и Государственной программе Информационное общество (2011–2020 годы) в качестве одного из приоритетных направлений развития информационных технологий указано «противодействие использованию информационных технологий в целях угрозы национальным интересам России, включая обеспечение безопасности функционирования информационно-телекоммуникационной инфраструктуры и информационных и телекоммуникационных систем»[119].

Повышение статуса Российской Федерации в международном сообществе, которое происходит с начала текущего столетия, требует от нашей страны

---

[117] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция Генеральной Ассамблеи ООН № A/RES/64/25 от 2 декабря 2009 года [Электронный ресурс]. – Режим доступа: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/463/35/PDF/N09463 35.pdf?Open Element. (дата обращения: 19.02.2014)

[118] Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 7 февраля 2008 г. № Пр-212) // http://sd6.uchebalegko.ru/docs/95900/index-8776.html; Государственная программа Российской Федерации «Информационное общество (2011–2020 гг.)», утв. распоряжением Правительства Российской Федерации от 20 октября 2010 г. № 1815-р Гл 2. // www.consultant.ru. (дата обращения: 04.05.2013)

[119] Там же.

развиваться такими же трендами и темпами, как и другие великие державы и высоко развитые индустриальные государства или даже, на некоторых направлениях, опережать их.

При этом необходимо учитывать возрастающую конкуренцию в международном сообществе и особенно – в группе его лидеров. Кроме того, сами лидеры делятся на старые великие державы и новые восходящие страны – гиганты. «Старые государства, – пишет С. Караганов, – и их институты (Организация экономического сотрудничества и развития (ОЭСР) – очевидно устаревший клуб развитых держав, тот же МВФ) будут бояться убыстрения потери статуса и позиций. Новые лидеры – те же Китай, Индия, – наслаждаясь вновь обретенным после веков подавления Западом полным суверенитетом, будут опасаться его ограничения»[120].

При данных обстоятельствах трансформация политики безопасности, в соответствии с новейшими требованиями и с условиями глобального развития как на международном, так и на национальном уровне, является одной из стратегических задач развития нашей страны и подержания ее статуса на мировой арене. При этом следует учитывать, что в сфере политики безопасности происходят существенные изменения объективного характера, связанные с расширением ее информационной составляющей.[121]

Информационная безопасность представляет собой достаточно сложное явление, что необходимо учитывать при формировании политики безопасности в целом. В информационной безопасности следует выделить три основных измерения – отраслевое, национальное и международное.

Специальное измерение связано с информационной безопасностью как процессом обеспечения функционирования собственно информационной сферы. В данном случае информационная безопасность носит скорее технический характер. Она связана, в первую очередь, с поддержанием устойчивого

---

[120] Караганов С. А. Россия в мире: Противоречие противоречий // Ведомости. 2012. 16 октября. С. 4.
[121] Государственная программа Российской Федерации «Информационное общество (2011–2020 гг.)», утв. распоряжением Правительства Российской Федерации от 20 октября 2010 г. № 1815-р Гл 2. // www.consultant.ru. (дата обращения: 04.05.2013)

функционирования информационной инфраструктуры. Защита осуществляется от технических сбоев; неумышленных воздействий, наносящих вред стабильной работе; попыток несанкционированного доступа, внедрения вредоносных программ и тому подобное.

Национальное измерение информационной безопасности имеет более широкий характер. В связи с этим П. А. Шариков пишет: «Информационные технологии нашли широкое применение практически во всех сферах национальной безопасности; с этим связана актуальность защиты информационных ресурсов. Воздействие на информацию или информационную инфраструктуру иной раз имеет катастрофические последствия на ту сферу, в которой они применяются»[122]. Таким образом, при более широком измерении информационной безопасности не в отраслевом масштабе, а в масштабе всей страны она может рассматриваться как важный элемент обеспечения национальной безопасности.

В наши дни информационные ресурсы и информационное пространство государства подвергаются воздействию из-за рубежа – со стороны субъектов глобального информационного пространства, которые находятся не только в сопредельных государствах, но и на других континентах.

«Глобализация экономики, информатизация международных отношений, – отмечает С. В. Кортунов, – создают беспрецедентные возможности для развития, но одновременно делают мировую систему уязвимой для терроризма, применения ОМУ, информационного оружия»[123].

Итак, в процессе глобализации возрастает значение международного измерения информационной безопасности. Угрозы, исходящие для национальной безопасности из глобального информационного пространства, становятся все более серьезными в военно-политическом плане и все более сложными в технологическом аспекте (Рисунок 1).

Одним из важных направлений трансформации политики безопасности

---

[122] Шариков П. А. Эволюция государственной стратегии в сфере информационной безопасности // США – Канада. Экономика, политика, культура. № 12. Декабрь 2009. С. 96.

[123] Кортунов С. В. Мировая военно-политическая ситуация. Год 2025 // Международная жизнь. 2010. № 3. С. 95.

современной России является органичное включение в нее процесса обеспечения информационной безопасности как одного из базовых системообразующих элементов. Данная деятельность должна носить комплексный характер и сочетать в себе все три основных измерения информационной безопасности: отраслевое, национальное и международное. Соотношения между этими измерениями носит динамический характер и может изменяться в зависимости от ситуации, связанной с внутренним и внешним развитием страны.

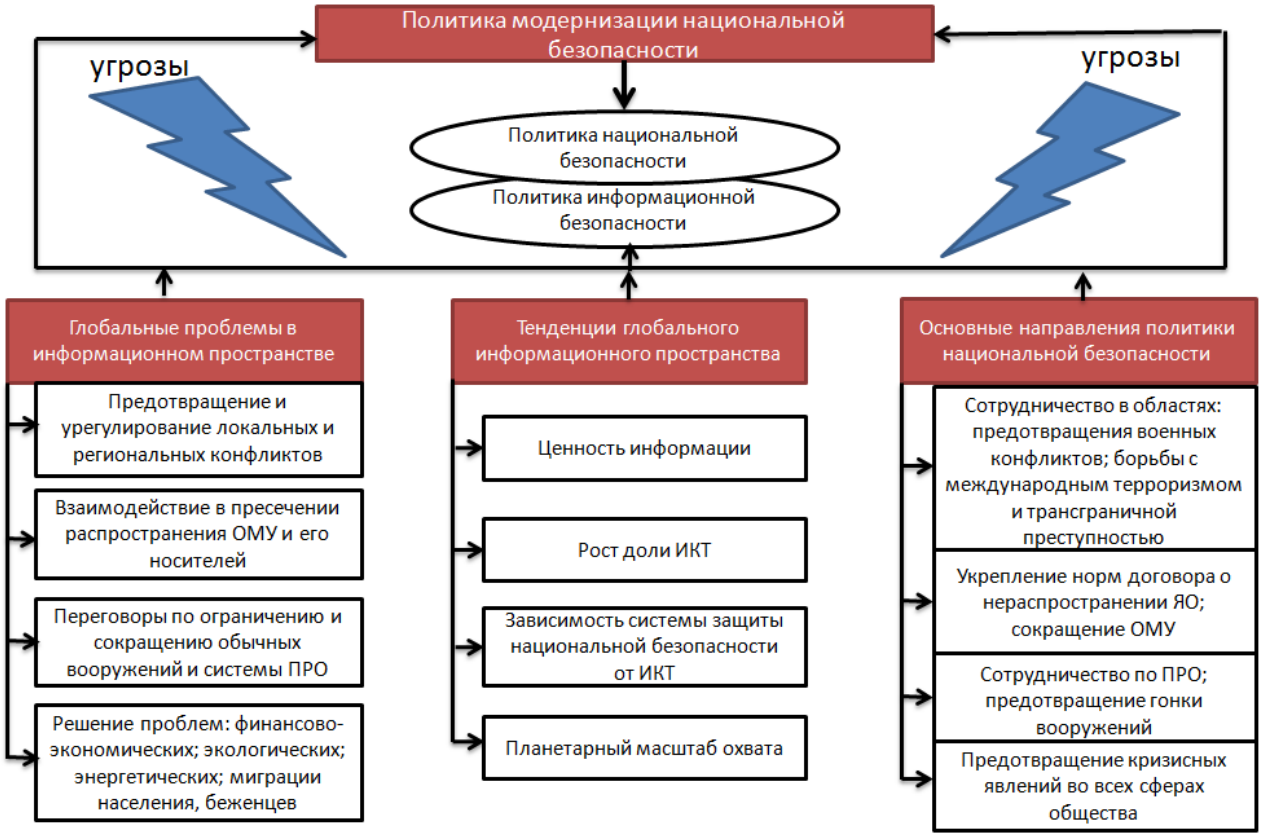


Рисунок 1 – Политика национальной безопасности в тенденциях современного глобального информационного пространства

1.3. Военно-политическая глобализация как фактор модернизации национальной безопасности

В современных условиях глобализация превратилась в основную тенденцию мирового развития. Этой тенденции присущи собственная явно

выраженная специфика и определенные противоречия, отличающие ее от других направлений развития мирового сообщества.

Под глобализацией, как правило, понимают изменения мирового масштаба, происходящие во всех основных сферах жизнедеятельности мирового сообщества и в системе международных отношений.

Многие авторы обращают внимание на многомерность, разноплановость и, одновременно, на взаимосвязанность и взаимодействие процессов глобализации. Они рассматривают этот феномен в более широком контексте. Например, Д. Хелд, А. Макгрей, Д. Голдблат и Дж. Перратон, авторы широко известного фундаментального труда «Глобальные трансформации, в данной связи пишут: «Глобализация может быть осмыслена как расширение, углубление и ускорение взаимосвязанности и взаимозависимости глобального масштаба во всех аспектах современной общественной жизни: от культуры до криминала, от финансов до духовности.

Так, компьютерные программисты в Индии предоставляют услуги в режиме реального времени для своих работодателей в Европе и США – в то время как выращивание опийного мака в Бирме может быть связано с наркоманией в Берлине или Белфасте. Приведенные примеры иллюстрируют, каким образом современная глобализация соединяет деятельность социальных групп в одном регионе мира с событиями, происходящими на другом континенте.»[124].

Глобализация оказывает непосредственное и самое существенное влияние на развитие военно-политической сферы в современном мире. Это влияние многопланово и противоречиво – как и сам процесс глобализации.

С одной стороны, глобализация современного международного сообщества ведет к повышению конкуренции на мировой арене, прежде всего, среди высоко индустриально развитых государств и других субъектов международных отношений. В этих условиях силовой фактор, связанный с обладанием государством технически оснащенных на уровне мировых стандартов и хорошо

[124] Held D., McGrew A., Goldblatt D., Perraton J. Global Transformation. Politics, Economics and Culture. Cambridge.: Polity Press, 2000. P. 2.

подготовленных вооруженных сил становится важным аргументом, позволяющим защитить национальные интересы, если конкурентная борьба начинает приобретать формы жесткого противостояния.

С другой стороны, процесс глобализации оказывает воздействие непосредственно на военно-политическую сферу как в мировом, так и национальном масштабах. На это явление обращают повышенное внимание исследователи проблем глобального развития, связанных с военными и политическими процессами в современном мире.

Одни из них акцентируют внимание на инновационных и научно-технических аспектах влияния глобализации на развитие военно-политической области. Речь идет о том, как изменившиеся под воздействием глобализации условия развития вооруженных сил (прежде всего переход современных армий на массовое использование высокотехнологичных систем вооружения) повлияли на основы функционирования и организации военной сферы государства, деятельность его учреждений.

Так, профессор университета Уорвик (Великобритания) Я. А. Шольте пишет: «Технологии, распространяемые в процессе глобализации, тесно связаны различными способами с развитием военной сферы. Например, телефон был использован на поле боя через два года после его изобретения. Кроме того, радио и лазеры вскоре после их появления стали широко использоваться в военных целях. Компьютерные сети были впервые разработаны в США для американских вооруженных сил в 1969 г. и стали одним из ключевых инструментов современной войны для ведущих держав.

Будущие военные операции, которые будут осуществлять наиболее могущественные державы, вполне могут свестись к вторжению в компьютерные системы государства-противника с целью захвата его киберпространства»[125].

Другие эксперты в первую очередь обращаются к анализу взаимосвязи глобализации и расширения геополитических пространств для военной деятельности или военного контроля, включая увеличение масштабов

[125] Scholte J.A. Globalization: A Critical Introduction. N.Y.: Palgrave Macmillan, 2005. P. 283.

потенциальных театров военных действий, вплоть до вынесения их в космическое пространство. Так, западные военные аналитики пытаются оправдать необходимость сохранения НАТО за счет расширения масштабов деятельности и глобализации статуса этой организации.

В частности, американский исследователь П. Уоррен в своей работе «История альянса и будущее НАТО» доказывает, что по мере своего развития Северо-Атлантический союз превратился в «гибридный» многосторонний альянс, решающий задачи как в сфере обороны, так и в сфере безопасности, причем с выраженным идеологическим компонентом. Именно это и позволило ему сохранить свой статус, когда после окончания «холодной войны» он лишился, в лице СССР, своего основного военного противника.

Надо отметить, что в подобных случаях, теряя смысл своего дальнейшего существования, оборонительные союзы обычно распадаются. Тот факт, что данный альянс сохранился, несмотря на изменение международной обстановки, предопределил смену его функционала, пересмотр целей и задач, а также глобализацию статуса[126].

Российские эксперты отмечают, что глобальные устремления НАТО просматриваются в его попытках играть значимую роль не только в вопросах обороны, предотвращения вооруженных конфликтов или террористических атак, но и в вопросах, которые традиционно относятся скорее к энергетической и экологической безопасности и не имеют явно выраженной военной составляющей[127].

Наибольший интерес для изучения влияния глобализации на военно-политическую сферу в контексте обеспечения национальной безопасности, включая такую ее важную составляющую, как информационная безопасность, представляет собой исследование таких проявлений глобализации в развитии военной составляющей современной мировой политики, как борьба с международным терроризмом в условиях глобального информационного

[126] Цит. по: Ермаков С. М. Трансформация НАТО после Лиссабонского саммита 2010 г.: от обороны территории к защите всеобщего достояния // Проблемы национальной стратегии. 2011. № 4. С. 110–111.
[127] Там же. С. 111.

общества, особенности современных военных конфликтов, трансформация современных арсеналов ведения войны, военные операции в глобальном информационном пространстве, глобализация и ядерное оружие.

Одной из негативных сторон процесса глобализации является, то, что этот процесс охватил криминальную сферу и способствовал, в частности, возникновению таких явлений, как международный терроризм, получивший глобальное распространение, не признающий ни государственных границ, ни правовых и моральных норм.

В последнее время борьба с международным терроризмом превратилась в одну из острейших глобальных проблем современности, связанных со сферой международных отношений. Эта трансформация обусловлена, по мнению российских исследователей, следующими причинами.

Во-первых, международный терроризм, к сожалению, получает все более широкое распространение в планетарном масштабе. Он проявляется в регионах, где многие десятилетия имеют место международные конфликты (например, Ближний Восток и Южная Азия). Однако, от этого опасного явления оказались не застрахованы и наиболее развитые и благополучные государства (в частности, США и Западная Европа).

Во-вторых, международный терроризм представляет собой серьезную угрозу для безопасности отдельных государств и всего мирового сообщества в целом. Ежегодно в мире совершаются сотни актов международного терроризма, а скорбный счет их жертв составляет тысячи убитых и искалеченных людей.

В-третьих, для борьбы с международным терроризмом недостаточно усилий одной великой державы или даже группы высокоразвитых государств. Преодоление международного терроризма как обостряющейся глобальной проблемы требует коллективных усилий большинства государств и народов на нашей планете, всего мирового сообщества.

В-четвертых, все более явной и наглядной становится связь современного феномена международного терроризма с другими актуальными глобальными проблемами современности. В настоящее время международный терроризм

должен рассматриваться как важный элемент всего комплекса общечеловеческих, глобальных проблем[128].

Международный терроризм имеет свои специфику и особенности, которые ведут к тому, что преступники нередко оказывают негативное влияние на развитие политических процессов, происходящих на планете, создают напряженность в мировой политике, существенно ухудшают состояние глобальной безопасности в целом и национальной безопасности ряда государств, включая и ведущие державы современности. Рассмотрим более подробно наиболее важные особенности и отличительные черты современного международного терроризма.

В первую очередь необходимо подчеркнуть, что проблема международного терроризма затрагивает жизненно важные и весьма уязвимые сферы функционирования международного сообщества и обществ отдельных стран – политику и экономику, транспорт и энергетику, национальные и религиозные отношениями и тому подобное. В настоящее время исследователи выделяют несколько основных направлений террористической деятельности: политический, этнический, религиозный, криминальный, экологический терроризм и др.

Для политического террора характерно достижение, прежде всего, политических, социальных или экономических изменений внутри того или иного государства. Политический террор нацелен также на подрыв межгосударственных отношений и международной стабильности.

Этнический терроризм преследует цели, связанные с изменением государственного строя и административно-территориального устройства государства в целом или правового статуса какого-либо входящего в данное государство территориального образования. Часть этнического терроризма имеет явные сепаратистские устремления к созданию новых государств – за счет расчленения уже существующих.

---

[128] Косов Ю. В. Международный терроризм как глобальная проблема // Социология войны и мира. Материалы «круглого стола»/под ред. П. А. Цыганкова. М.: Альфа-М, 2006. С. 135..

Терроризм этнонационального толка может переплетаться с другими формами незаконной насильственной деятельности: партизанской войной, восстаниями, мятежами и попытками государственного переворота.

Религиозный терроризм обоснован преимущественно религиозной аргументацией, хотя цели террористов чаще всего носят конкретный политический характер. Мотивация террористов, непосредственно совершающих насильственные действия, также базируется на религиозной основе. Побудительными мотивами для такой деятельности является религиозный фанатизм, толкающий людей даже на самоубийство. В современном мире этнический и религиозный терроризм часто пересекаются[129].

Терроризм криминальной природы выстраивается в какой-либо преступной сфере, где осуществляется незаконный бизнес. К таким сферам обычно относят: наркобизнес, торговлю людьми, незаконный оборот оружия и ядерных материалов, контрабанду и тому подобное.

Экологический терроризм связан с применением насильственных методов группами, протестующими против научно-технической революции , разрушения природы, распространения атомной энергетики и строительства других ядерных объектов и так далее.

Международный терроризм достаточно трудно поддается анализу и прогнозированию. Достаточно часто к методам террора обращаются психически неуравновешенные личности или политические деятели, имеющие склонность к насилию и непомерные амбиции. В XXI веке террористическая деятельность все более усложняется. Совершаемые террористические акты представляют собой преступления против человечности и вызывают всеобщее возмущение.

Таким образом, международный терроризм в наши дни вполне обоснованно рассматривается как угроза глобальной и национальной безопасности многих государств. Как известно, после беспрецедентных террористических актов 11 сентября 2001 года в Нью-Йорке была организована международная антитеррористическая коалиция. В состав этой коалиции вошли

[129] Ланцов С. А. Террор и террористы. Словарь. СПб: Изд-во С.-Петербургского ун-та, 2004. С. 127–130, 170–171.

десятки государств, что раньше имело место только в случае крупных вооруженных конфликтов и войн.

В данных условиях глобальная проблема международного терроризма не может рассматриваться только как самостоятельный феномен. Она начала превращаться в важную составную часть более общей проблемы глобальной безопасности. Непосредственно международный терроризм и борьба с ним представляют собой проявление процесса военно-политической глобализации.

Выше были рассмотрены основные течения международного терроризма, которые уже имеют достаточно длительную историю и в отношении которых накоплен значительный опыт борьбы с ними. В последние годы наблюдается формирование принципиально нового направления террористической деятельности, которое получило название «информационный терроризм», или «кибертерроризм».

Эксперты отмечают, что информационный терроризм (кибертерроризм)[130] следует отличать от информационного криминала (киберпреступности).

Киберпреступления связаны с корыстным характером действий правонарушителей. Эти преступления обычно носят разовый характер и направлены против определенного субъекта информационного пространства. В частности, злоумышленники могут противоправно вмешиваться в работу компьютерных сетей, несанкционированно модифицировать компьютерные данные, а также совершать иные противоправные деяния в киберпространстве.

Так, Е. Старостина следующим образом характеризует рассматриваемое различие: «Информационный терроризм («кибертерроризм») отличается от указанных форм воздействия на киберпространство прежде всего своими целями,

[130] Информационный терроризм за последние время превратился в одно из наиболее опасных проявлений высокотехнологического терроризма, а информационные технологии стали его новой базой. Некоторые исследователи определяют информационный терроризм как сознательное злоупотребление цифровыми информационными системами, сетями (или компонентами этих систем либо сетей) в целях, которые способствуют осуществлению террористических операций (или актов). Термин «кибертерроризм», в свою очередь, ввел в середине 1980-х гг. сотрудник американского Института безопасности и разведки Б. Колин; обозначал он террористические действия в виртуальном пространстве. Тогда этот термин использовался лишь для прогнозов на будущее. Сам автор термина предполагал, что о реальном кибертерроризме можно будет говорить не раньше, чем в первые десятилетия XXI в. (Подробнее см.: Туронок С. Г. Информационный терроризм: выработка стратегии противодействия // Общественные науки и современность. 2011. № 4. С. 131–133.

которые остаются свойственными политическому терроризму вообще. Средства осуществления информационно-террористических действий могут варьироваться в широких пределах и включать все виды современного информационного оружия.

В то же время, тактика и приемы его применения существенно отличаются от тактики информационной войны и приемов информационного криминала. Главное в тактике информационного терроризма состоит в том, чтобы террористический акт имел опасные последствия, стал широко известен населению и получил большой общественный резонанс. Как правило, требования сопровождаются угрозой повторения акта без указания конкретного объекта»[131].

Таким образом, международный терроризм активно действует в глобальном информационном пространстве, не признавая государственных границ, не имея ни национальной, ни религиозной принадлежности. В данной связи крайне актуальной становится проблема обеспечения информационной безопасности, как одной из важных составляющих национальной безопасности государства.

Для выполнения этой задачи требуется серьезная модернизация систем обеспечения национальной безопасности современных государств, включая Россию. Эта модернизация должна учитывать не только сегодняшние, но и перспективные результаты внедрения инновационных технологий, изменяющих глобальное информационное пространство.

Особое беспокойство вызывает то, что экстремистские группировки, сепаратистские силы, проповедники идей, противоречащих общечеловеческим ценностям, стремятся интенсивно использовать современные передовые информационные технологии для пропаганды своей идеологии и достижения своих целей.

Например, в настоящее время в Интернете находятся сайты практически всех более или менее крупных исламистских организаций, в том числе

[131] Старостина Е. Терроризм и кибертерроризм: угроза международной безопасности // Центр исследования компьютерной преступности. Интернет-издание (www.crime-research.ru). (дата обращения: 17.04.2013)

радикального толка («Международный исламский фронт», «Армии освобождения Косово», «Исламская группа» и др.).

Большинство таких сайтов образуют специфическую подсеть в Интернете, главные цели которой – это информационно-пропагандистское воздействие и организационная деятельность. Кроме того, Интернет используется радикальными группировками в качестве средства связи.[132]

Необходимо отметить, что террористы и экстремисты стремятся захватить и использовать для достижения своих преступных целей информационное пространство даже в тех странах, где оно, в силу социально-экономической отсталости этих государств, находится на начальной стадии формирования.

Например, в Афганистане, где радио, печать и мечеть остаются основными источниками распространения информации, движение «Талибан» использует традиционные каналы воздействия на население.

Основной рупор пропаганды талибов – подпольное «Радио «Шариат» (Radio Shariat). Кроме радио, традиционная пропаганда «Талибана» включает в себя так называемые ночные письма или листовки, которые призывают афганцев жертвовать деньги на джихад и вредить коалиционным силам.

Талибские пропагандисты понимают, что одними угрозами и призывами к джихаду, при всей их эффективности, информационную войну не выиграть. Они, перехватив лозунги коалиционных войск в Афганистане, стали выступать за улучшение социально-экономического положения страны, избавление ее от коррупции, прозрачность в управлении на всех уровнях, расширение прав женщин.

Контрпропагандистская кампания Вашингтона в Афганистане и Пакистане включает в себя такие направления, как информационная война против талибов и «Аль-Каиды», обучение социально-профессиональных групп и проведение мероприятий против медиаджихада в Интернете. Однако, представители армии США, включая бывших главнокомандующих коалиционными войсками (в

[132] Там же.

частности, генерала Д. Барно), неоднократно признавали, что США проигрывают талибам пропагандистскую войну[133].

Важным направлением воздействия глобализации на военно-политической сферу мирового сообщества и на процессы обеспечения международной безопасности, кроме международного терроризма, являются военные конфликты в современном мире. В наши дни эти конфликты приобрели новые особенности и черты.

В последние годы, как правило, происходят межгосударственные вооруженные конфликты, в которые оказываются втянутыми, с одной стороны, государство (или коалиция государств), обладающее значительным военным потенциалом, а с другой – страна, военный потенциал который крайне мал. В результате такого столкновения на первом этапе, который обычно является достаточно быстротечным, победа достается обладателям военной мощи.

Однако, это не означает окончание войны. Проигравшая сторона переводит вооруженный конфликт на стадию партизанской войны, которая может продолжаться достаточно долго.

Так, эксперт Российского совета по международным делам Н. Мендкович, анализируя вооруженные конфликты первого и начавшегося второго десятилетия XXI века, приходит к следующему выводу: «Опыт иракской войны показал, что армия-победительница уже после быстрой военной победы над армией противника может столкнуться с наибольшими трудностями, а именно: с сопротивлением мобильных отрядов партизан. По этому сценарию развивалась и ситуация в Афганистане. По всей видимости, что-то подобное повторится и в Мали, пусть и в меньших масштабах»[134].

Таким образом, подавляющее военное преимущество Соединенных Штатов в Ираке оказалось недостаточным для разгрома партизанских формирований в относительно короткий срок. В итоге, американской армии, несмотря на

---

[133] Подробнее о событиях в информационном пространстве Афганистана см.: Цветкова Н.А. Информационная война талибов: Вашингтон в обороне // Азия и Африка сегодня. 2013. Январь. № 1. С. 10–16.

[134] Мендкович Н. Ирак: десять лет спустя. 23 марта 2013 г. // http://russiancouncil.ru/inner/?id_4=1584#top. (дата обращения: 25.05.2013)

массированное преимущество авиации, пришлось проводить наземные операции антипартизанского характера на всей территории страны, что потребовало ввода дополнительных контингентов.

Как отмечают военные эксперты, интенсивная партизанская война в Ираке велась уже в первый год оккупации. В 2003 году оккупационные власти регистрировали 10–35 террористических атак в день, в 2004 году – 25–80, в 2005 году – 65–90. В общей сложности, в 2003–2005 гг. погибли почти 2 400 иностранных военных и до 40 000 иракцев. Причем эта оценка потерь среди мирного населения, скорее всего, является заниженной: многие исследователи называют большее число прямых и косвенных жертв боевых действий[135].

По аналогичному сценарию развивалась ситуация и в Афганистане. В Мали, после ввода Францией своих вооруженных сил в эту западно-африканскую страну, широкомасштабная война быстро была прекращена вследствие их военных успехов. Однако, по мнению специалистов, многие отряды исламистов, по всей видимости, уклонились от боевых столкновений с французской армией для того, чтобы впоследствии организовать партизанскую борьбу.

«Вместе с тем, не следует забывать, что страна уже вступила в партизанскую фазу войны с терроризмом. В рамках этого этапа боевых действий французской армии и ее союзникам придется решать в Мали принципиально иные задачи, о сложности которых судить пока рано»[136].

В то же время, современные военные конфликты, в качестве важной составной части, включают в себя информационное противоборство конфликтующих сторон в региональном информационном пространстве. Пример такого противоборства был рассмотрен ранее – когда обсуждалась информационная война талибов в Афганистане против коалиционных сил.

Кроме того, военные конфликты порождают и информационные войны в глобальном информационном пространстве. Ведущая держава, участвующая в конфликте, для ведения такой войны использует свои мощные информационные

---

[135] Там же.

[136] Мендкович Н. Есть еще порох в пороховницах? РСМД. 25 февраля 2013 г. // http://russiancouncil.ru/inner/?id_4=1440#top. (дата обращения: 24.05.2014)

ресурсы. Обычно партизаны и другие вооруженные формирования, борющиеся с такой державой, явно имеют гораздо более ограниченные информационные возможности. Однако, благодаря Интернету и другим современным информационно-коммуникационным средствам, их позиция может быть достаточно четко обозначена в глобальном информационном пространстве.

В современных локальных вооруженных конфликтах происходит существенная трансформация современных арсеналов ведения войны. Обычные вооружения применяются в сочетании с информационными средствами и методами ведения враждебных действий. Например, заместитель директора Института США и Канады РАН, известный российский военный эксперт П. С. Золотарев следующим образом описывает три основных этапа «идеального, с позиции нападающей стороны, сценария локального конфликта».

На первом этапе организуется и проводится информационная операция стратегического масштаба. Ее цели – дискредитировать политическое руководство «проблемной страны» на международном и внутреннем уровнях, обозначить и обеспечить поддержку оппозиционных сил.

На втором этапе дестабилизируется ситуация внутри «проблемной страны» – с тем чтобы к власти пришли нужные оппозиционные силы. При необходимости проводится специальная кампания по дискредитации или физическому уничтожению действующего политического руководства.

Третий этап связан с открытым использованием военной силы. Он зависит от успеха двух предшествующих. Если к власти в «проблемной стране» удалось привести нужные политические объединения, то третий этап оказывается излишним; если это не удалось, то обычно прибегают к применению военной силы. Международное сообщество следует убедить в необходимости военной операции[137].

Таким образом, очевидно, что вооруженные действия и информационные операции взаимно дополняют друг друга. В современных условиях они

[137] Золотарев П. С. Глобальное измерение войны // Россия в глобальной политике. 2010. № 1. С. 56.

фактически составляют единый комплекс мер, которые применяют ведущие державы в современных региональных и локальных вооруженных конфликтах.

Соотношение методов и способов воздействия и привлекаемых сил, входящих в этот комплекс, зависит от конфигурации конкретного конфликта. В наши дни такие конфликты имеют значительные разнообразие и специфику. «За последнее десятилетие (2000 – 2012 гг.) только три из 30 крупных вооруженных конфликтов, – пишет А. Г. Арбатов, – были межгосударственными (между Индией и Пакистаном, Эфиопией и Эритреей и вооруженная интервенция США в Ираке в 2003 году). Все остальные носили смешанный характер с прямым или косвенным вмешательством извне…

При этом целью вмешательства была как поддержка повстанцев против центрального правительства (Ливия, Сирия), так и помощь центральному правительству в подавлении вооруженной оппозиции (Ирак, Афганистан). Нередко за спиной локальных конфликтующих сторон стоят крупные державы и корпорации, соперничающие за экономическое и политическое влияние, получающие доход от поставок наемников, вооружений и боевой техники»[138].

Итак, следует отметить, что военно-политическая глобализация выступает ключевым фактором в процессе модернизации системы национальной безопасности Российской Федерации (Рисунок 2).

[138] Арбатов А. Г. Угрозы реальные и мнимые. Военная сила в мировой политике начала XXI в. // Россия в глобальной политике. 2013. Март–апрель. Т. 11. № 2. С. 16.

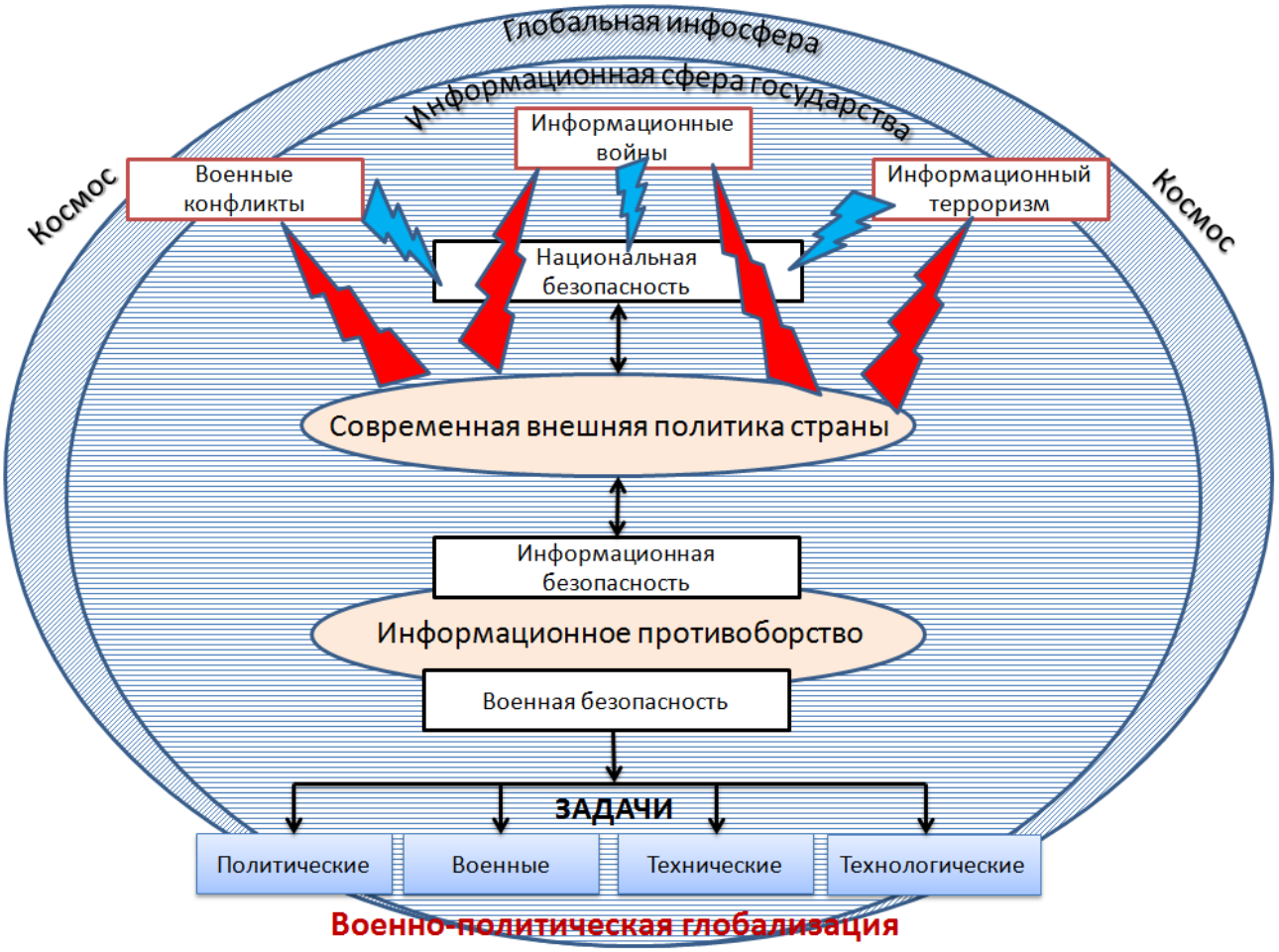


Рисунок 2 – Военно-политическая глобализация – ключевой фактор модернизации национальной безопасности

Во-первых, глобализация делает прозрачными государственные границы, ведет к созданию общих глобальных пространств безопасности в основных сферах жизнедеятельности человеческого сообщества: прежде всего в сфере экономической безопасности и др.

Во-вторых, возникают пространства, которые выходят за пределы нашей планеты. Таким феноменом в первую очередь следует считать пространство воздушно-космической безопасности.

В-третьих, в последнее время появились принципиально новые виртуальные пространства, которые в процессе своего развития образовали глобальное информационное пространство. Формирование этого пространства поставило вопрос обеспечения информационной безопасности, которую следует

рассматривать как важную составную часть системы поддержания национальной безопасности.

В «Стратегии национальной безопасности Российской Федерации» в данной связи при анализе перспективных угроз и проблем мирового развития, с которыми столкнется и Россия, отмечается усиление глобального информационного противоборства в ближайшем будущем. В документе написано, что «усилится глобальное информационное противоборство, возрастут угрозы стабильности индустриальных и развивающихся стран мира, их социально-экономическому развитию и демократическим институтам»[139].

Таким образом, информационная безопасность в современных условиях является важнейшим фактором в системе обеспечения стабильного и устойчивого развития современного государства.

Решение вопросов поддержания информационной безопасности связано напрямую с обеспечением экономического благополучия и демократического управления в рамках современного государства. Поэтому при развитии и модернизации современной системы национальной безопасности России, необходимо самым серьезным образом принимать в расчет ее информационную составляющую.

Информационный компонент системы обеспечения национальной безопасности имеет явно выраженное информационное измерение. Это измерение невозможно игнорировать в современных условиях. От глобального информационного пространства невозможно отгородиться ни «железным занавесом», как это бывало в прошлые времена, ни каким-либо другим искусственным препятствием.

Необходимо ориентировать силы, обеспечивающие национальную безопасность России и на информационном направлении, на активное участие в процессах формирования и развития глобального информационного

---

[139] Стратегия национальной безопасности Российской Федерации до 2020 г. Утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537 // Российская газета. 2009. 19 мая. Гл. 1. Ст. 10.

пространства, в том числе и в той его области, которая связана с поддержанием информационной безопасности.

Важным направлением обеспечения национальной безопасности России в информационном измерении является использование в этих целях международного права. Информационное противоборство в современных условиях следует рассматривать как наиболее вероятную форму агрессивного воздействия на российское информационное пространство с целью нанесения конкретного ущерба.

Для информационного противоборства в современных условиях характерны следующие основные черты: скрытый, неявный характер проявления, реализация многих действий при помощи сетевой среды, осуществление в рамках глобального информационного пространства.

Скрытые, или неявные формы информационного противоборства разнообразны. Действия, нацеленные на разрушение единства общества в политическом, социальном и национальном планах, могут быть завуалированы под информационные материалы, развлекательные шоу или познавательные программы.

Некоторые исследователи уже обращают внимание на такой феномен, как распространение слухов с помощью современных информационно-коммуникационных систем, который уже может представлять существенную угрозу безопасности общества, исходящую из информационного пространства.

Так, Е. М. Куликов обращает внимание на обстоятельства, согласно которым, «приобретает важность и практическую направленность дальнейшая разработка методологических и методических аспектов проведения мониторинговых социологических исследований в сети Интернет с целью контроля над процессом генезиса и распространения слухов. В противном случае мы столкнемся с угрозой мощного информационного воздействия на население,

так как сейчас слухи в Интернете распространяются во много раз быстрее, чем традиционным способом, известным с древнейших времен»[140].

Таким образом, информация, исходящая из различных источников от программ и материалов, распространяемых СМИ до слухов, может служить оружием враждебного информационного воздействия. Наиболее эффективным средством распространения информации в наше время стали сетевые коммуникационные системы, базирующиеся на глобальной сети Интернет. Они стали таковыми естественным путем под воздействием объективных факторов.

Однако, силы, вовлеченные в информационное противоборство в современном мире, быстро поняли значимость информационных сетей для проведения соответствующих конфронтационных действий. В настоящее время информационные сети представляют собой широкое поле для информационного противоборства как в локальном, так и в глобальном масштабах.

Итак, использование как глобальных информационных сетей, так и глобального информационного пространства в целом придало рассматриваемому противоборству поистине всемирный глобальный характер. Данное обстоятельство важно учитывать в процессе модернизации современной системы национальной безопасности. Данная система должна опираться не только на внутреннее право Российской Федерации, но и широко использовать международное право в области информационной и кибербезопасности.

Следует не только ориентироваться на нормы и принципы международного права, но и, поскольку право информационной безопасности – достаточно новый международно-правовой институт, необходимо активно участвовать в его формировании, кодификации и развитии. Таким образом, Россия сможет укрепить международно-правовые основы процесса обеспечения информационной безопасности как на национальном, так и на глобальном уровнях.

В данной связи А. К. Жарова отмечает, что «разнообразие сторон в информационном противоборстве, его фактическая неявность, сетевая среда и

---

[140] Куликов Е. М. Перспективы противодействия слухам в глобальной сети Интернет в целях обеспечения информационной безопасности // Власть. 2011. № 3. С. 68.

глобализация действий обязывает выработать новые взгляды на роль и место права в регулировании информационных противоборств»[141].

Военно-политическая глобализация требует учитывать планетарный масштаб угроз и проблем, возникающих при обеспечении национальной безопасности, особенно в таком ее сегменте, как информационная безопасность.

Вопросы международно-правового обеспечения действий России в сфере информационной безопасности, как и другая деятельность в этом направлении, связанная с решением задач политического, военного и технического характеров, должна строиться с учетом глобального контекста. Эти вопросы будут рассмотрены более подробно в последующих главах.

* * *

Итак, завершая данную главу, следует обратить внимание на следующие положения, вытекающие из проведенного исследования.

Во-первых, в последние несколько десятилетий категория безопасность приобрела качественно новое содержание. Развитие мирового сообщества в наше время характеризуется возникновением и обострением глобальных проблем, имеющих политическую, экономическую, экологическую, энергетическую и иную природу. Эти проблемы усложняются колоссальным научно-техническим прогрессом.

Взаимозависимость государств и регионов мира также постоянно возрастает. Этот процесс проявляется в создании мировых рынков и региональных общих экономических пространств, появлении оружия массового уничтожения, способного истребить все живое на планете, и других подобных явлениях.

Данные реалии мирового развития в современных условиях на первый план выдвинули проблему обеспечения безопасности в глобальном масштабе: то есть проблему обеспечения международной безопасности.

---

[141] Жарова А. К. Сущность и структура информационного противоборства // Государство и право. 2009. № 2. С. 54.

Во-вторых, упрочение позиций нашей страны в современном глобальном мире и надежное обеспечение ее национальной безопасности связано с формированием и контролем над развитием такой ведущей тенденции мировой политики нашего времени, как повсеместное распространение новых информационно-коммуникационных технологий.

Процесс информатизации в современном мире имеет глобальный характер, и ему еще присуще общецивилизационное значение. Информатизация как важнейшая и долговременная тенденция развития мирового сообщества находится в тесной взаимосвязи с другим подобным процессом всемирного масштаба – глобализацией.

В-третьих, международный статус России в современном мире в значительной мере базируется на ее существенной вовлеченности в процессы глобального развития на самом высоком уровне. Так, наша страна принимает активное участие в деятельности элитных и наиболее влиятельных международных институтов и организаций глобального масштаба, в которых она находится на первых ролях. Россия активно участвует в процессах поддержания международной безопасности и все в большей мере обеспечении глобальной информационной безопасности.

В-четвертых, как показал проведенный анализ, для процессов обеспечения национальной и международной безопасности в современных условиях характерны следующие тенденции: повышение значимости информации и знаний для поддержания безопасности; увеличение доли информационных коммуникаций, средств и продуктов, используемых в процессе обеспечения безопасности; зависимость современного прогресса в сфере защиты национальной и международной безопасности во многом от успехов в развитии информационных технологий и связанных с ними областей народного хозяйства.

В данной связи следует обратить особое внимание на формирование, на базе группы наиболее индустриально развитых стран, сферы высоких информационных технологий. Создание подобной сферы является серьезным глобальным вызовом для национальной безопасности Российской Федерации.

В-пятых, принципиально важное направление трансформации политики безопасности современной России представляет собой развитие процесса обеспечения информационной безопасности как одного из базовых элементов системы национальной безопасности нашей страны. Решение этой задачи следует решать комплексно: на основе органичного сочетания трех главных измерений информационной безопасности: отраслевого, национального и международного.

В-шестых, информационное противоборство, порождаемое обостряющейся конкуренцией между ведущими державами современного мира, все в большей мере будет распространяться на российское информационное пространство. Для данного противоборства характерны следующие основные черты: скрытый, неявный характер осуществления, реализация многих действий при помощи сетевой среды, реализация в рамках глобального информационного пространства. Серьезную опасность представляет и информационный терроризм.

В-седьмых, военно-политическая глобализация повышает значимость информационной безопасности в процессе обеспечения стабильности на национальном уровне. В данном процессе возрастает роль правового обеспечения действий России в сфере информационной безопасности, которая должна сочетаться с решением задач политического, военного и технического характеров с учетом их глобального контекста.

2. МОДЕРНИЗАЦИЯ СИСТЕМЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В КОНТЕКСТЕ ПОВЫШЕНИЯ ЗНАЧИМОСТИ ИНФОРМАЦИОННОЙ СОСТАВЛЯЮЩЕЙ

В современном мире нарастают противоречия геополитического и геоэкономического характеров, усиливается конкуренция между отдельными ведущими странами, группами государств и макрорегионами. Данные процессы протекают на фоне вступления человечества в новую фазу развития, связанную со становлением глобального информационного общества.

Так, известный российский специалист в области геополитики С. А. Караганов заявляет: «Я, к сожалению, абсолютно уверен, что взятый американцами курс на сдерживание России в духе «холодной войны» и даже на отбрасывание (не надо путать со сдерживанием ядерным) наклевывался уже в течение последних полутора лет. Это началось, когда США поняли, что Россия не пойдет, как там надеялись, в русле общезападной политики. Этот курс стал совершенно очевидным уже весной – осенью прошлого года»[142].

В данных условиях проблемы обеспечения национальной безопасности приобретают для Российской Федерации жизненно важный характер. В связи с этим требует модернизации и система национальной безопасности нашей страны. Во-первых, во время структурного кризиса 1990-х гг., который привел к резкому ограничению ресурсов и возможностей, сфера обеспечения национальной безопасности не получила должного развития.

Компенсация допущенного отставания осуществляется в наши дни. В данной связи модернизационный подход позволяет решить эту задачу быстрее и на качественно ином уровне, чем это было возможно два десятка лет тому назад.

Во-вторых, существенное изменение геополитической картины современного мира, связанное с усилением тенденции перехода к многополярному миру и стремлением США и их союзников сохранить мировой

[142] Шестаков Е. Мир становится все менее прозападным / Интервью с С. Карагановым // Российская газета. 2014. 24 апреля. С. 1, 10.

порядок, сложившийся в период монополярной системы международных отношений, увеличивает риски в обеспечении национальной безопасности Российской Федерации и международной безопасности в целом.

В-третьих, стремительное развитие информационно-коммуникационных технологий, создание глобального информационного пространства, коренным образом усилили значение информационной составляющей в обеспечении национальной безопасности. Инновационное развитие сил и средств обеспечения информационной составляющей национальной безопасности должно стать магистральным направлением модернизации всей системы национальной безопасности.

2.1. Динамика системных изменений национальной безопасности в XXI веке

Международные процессы в XXI веке отличаются высоким динамизмом и определенной противоречивостью. Большое влияние на них оказывают новейшие достижения научно-технического прогресса. В связи с этим возникают новые угрозы и вызовы национальной безопасности государств современного мира, в том числе и России.

В наше время Российская Федерация обладает развитой системой обеспечения национальной безопасности. Эта система базируются на положениях «Стратегии национальной безопасности Российской Федерации до 2020 г.», а также на других законодательных и нормативных актах. Данная стратегия разрабатывалась с учетом накопленного нашей страной опыта осуществления внешней и оборонной политики в период Второй Мировой войны, а также в годы «холодной войны» и во время кардинальных геополитических трансформаций системы международных отношений на рубеже XX и XXI веков.

Таким образом, система обеспечения национальной безопасности России, с одной стороны, постоянно развивается и совершенствуется с учетом конкретных исторических вызовов, обусловленных изменениями геополитической ситуации в

мире и в его отдельных регионах. С другой стороны, данная система сохраняет преемственность в своем развитии.

Современная система обеспечения национальной безопасности включает соответствующие силы и средства, необходимые для выполнения поставленных перед ней задач. Данная система в XXI веке претерпевает существенные динамичные изменения, обусловленные воздействием целого комплекса факторов, имеющих как социально-политическую природу, так и связанных с прогрессом в развитии современных технологий.

В значительной степени, политические и социальные факторы оказывают влияние на динамику изменений такого элемента рассматриваемой системы как «силы обеспечения национальной безопасности». К данным силам относят Вооруженные Силы Российской Федерации, другие войска, воинские формирования и органы, в которых федеральным законодательством предусмотрена военная и (или) правоохранительная служба, а также федеральные органы государственной власти, принимающие участие в обеспечении национальной безопасности государства на основании законодательства Российской Федерации»[143].

В систему обеспечения национальной безопасности Российской Федерации входит конституционный орган, который осуществляет координирующую деятельность в области обеспечения национальной безопасности. Данным органом является Совет Безопасности Российской Федерации, статус которого определен Конституцией Российской Федерации и Федеральным законом «О безопасности».[144]

Создание Совета Безопасности Российской Федерации позволило оперативно и адекватно отвечать на изменения и вызовы в сфере обеспечения безопасности как на глобальном уровне, так на региональном и национальном уровнях.

---

[143] Стратегия национальной безопасности Российской Федерации до 2020 год. Утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537 // Российская газета.. 2009. 19 мая. Гл. 1. Ст. 6.

[144] Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве [Электронный ресурс] / Министерство обороны России, 2011 г. – Режим доступа: http://ens.mil.ru/science/ publications/more.htm?id=10845074@cmsArticle. (дата обращения: 05.09.2012)

Предшественником российского Совета Безопасности следует рассматривать Совет Безопасности СССР, созданный 26 декабря 1990 года. Вскоре после этого события в России начался процесс формирования собственного Совета Безопасности, который завершился опубликованием Указа Президента Российской Федерации от 3 июня 1992 года № 547 «Об образовании Совета Безопасности Российской Федерации».

При формировании Совета Безопасности в нашей стране в определенной мере был учтен и зарубежный опыт создания Совета национальной безопасности (СНБ) Соединенных Штатов Америки, который был образован в 1947 году. Серьезная адаптация деятельности этого органа к современным условиям и вызовам XXI веке была проведена Президентом США Б. Обамой в начале его первого президентского срока. Президентская политическая директива № 1 Б. Обамы «Об организации системы Совета национальной безопасности», подписанная в феврале 2009 года, определяет новый состав СНБ, структуру его межведомственных органов, их функции и порядок работы. В этой директиве заявлено, что «СНБ будет основным форумом для рассмотрения вопросов политики национальной безопасности, требующих решения президентом, призванным консультировать главу государства и помогать ему в интеграции всех аспектов политики национальной безопасности – внутренних, внешних, военных, разведывательных и экономических (в сотрудничестве с национальным экономическим советом)»[145].

Участие СНБ США в политическом руководстве страной, согласно американской политической традиции, прежде всего, ориентировано на достижение сложных, многосторонних, межведомственных компромиссов по вопросам обеспечения национальной безопасности путем согласования и убеждения всех заинтересованных сторон.

В данной связи важно отметить, что Совет национальной безопасности играет роль «арбитра» в процессе принятия решений по проблемам безопасности

[145] Цит. по: Иванов С. Б. Структура и функции Совета национальной безопасности США // Зарубежное военное обозрение. 2013. № 4. С. 14.

и связанным с ними внешнеполитическим вопросам. Таким образом, проводится работа по оптимизации и координации действий различных государственных органов США перед лицом системных изменений в области глобальной и национальной безопасности.

Российский эксперт С. Иванов отмечает: «Одной из наиболее проработанных и устоявшихся форм участия СНБ в процессе выработки и проведения государственной политики США является стройная система «сквозного» межведомственного согласования, позволяющая значительно ускорить обычные процедуры длительного обращения документов между различными учреждениями некоторых других государственных учреждений и состоящая из нескольких уровней»[146].

Подобные координирующие государственные органы существуют и в других странах. Некоторые из них созданы раньше, чем в Российской Федерации. К таким органам следует отнести, например, Генеральный совет по обороне и безопасности при премьер-министре Франции, соответствующие государственные структуры в Турции, Иране и некоторых других странах.

Деятельность Совета национальной безопасности Турецкой республики регулируется на основе Конституции страны, Закона Турции «О Совете национальной безопасности Турции и Генеральном секретариате СНБ», принятого в 1983 году, и «секретной конституции», содержание которой является государственной тайной.

Этот конституционный орган играет важную роль в руководстве страной. В него входят президент, премьер-министр, министры обороны, внутренних и иностранных дел, а также высшее военное руководство. В соответствии с внесенной поправкой в конституцию, на пост генерального секретаря СНБ

[146] Иванов С. Б. Структура и функции Совета национальной безопасности США // Зарубежное военное обозрение. 2013. № 4. С. 15.

с 2004 года назначается гражданское лицо (ранее назначались высокопоставленные представители Генштаба).[147]

Высший совет национальной безопасности (ВСНБ) Исламской Республики Иран был создан в 1989 году – после внесения поправок в конституцию. Принципы его организации и полномочия подробно описаны ст. 176 Основного закона Ирана, в котором написано: «Для обеспечения национальных интересов и защиты Исламской революции, территориальной целостности и национального суверенитета создается Совет национальной безопасности под руководством Президента со следующими обязанностями:

1) определение политики страны в области обороны и безопасности страны в рамках общей политики, определенной лидером страны;

2) согласование политической, информационной, социальной, культурной и экономической деятельности в связи с общими мерами в области обороны и безопасности;

3) использование материальных и интеллектуальных возможностей страны для противодействия внутренней и внешней угрозе»[148].

В ряде постсоветских государств, с учетом мирового опыта и не без влияния российских политических реалий, для обеспечения национальной безопасности были созданы соответствующие конституционные органы. Так, уже в 1992 году организованы Совет национальной безопасности и обороны Украины (СНБО) и Совет Безопасности Республики Казахстан.

Функциями Совета национальной безопасности и обороны Украины являются:

1) внесение предложений Президенту Украины по реализации основ внутренней и внешней политики в сфере национальной безопасности и обороны;

---

[147] Турецкая республика. // Портал внешнеэкономической информации. Министерство внешнеэкономического развития Российской Федерации //http://www.ved.gov.ru/exportcountries/tr/about_tr/review_tr. (дата обращения: 21.02.2014)

[148] Конституция Исламской Республики Иран // http://read24.ru/fb2/konstitutsionnoe-sobranie-konstitutsiya-islamskoy-respubliki-iran/c (дата обращения: 21.02.2014)

2) координация и осуществление контроля за деятельностью органов исполнительной власти в сфере национальной безопасности и обороны в мирное время;

3) координация и осуществление контроля за деятельностью органов исполнительной власти в сфере национальной безопасности и обороны в условиях военного или чрезвычайного положения, а также в случае возникновения кризисных ситуаций, угрожающих национальной безопасности Украины[149].

Вслед за Россией и Украиной, подобные конституционные органы учредили и в ряде других постсоветских государств. В их числе следует назвать такие структуры государственной власти в новых независимых государствах, как Совет Безопасности Республики Казахстан, Совет безопасности Киргизской Республики, Высший совет безопасности Республики Молдова, Совет безопасности Республики Таджикистан.[150]

Таким образом, на рубеже XX и XXI веков проблемы обеспечения безопасности выдвинулись на первый план как в мировой политике, так и в деятельности органов власти и общественности ведущих государств современного мира.

В частности, А. Г. Санина отмечает: «Вследствие информатизации общества каждый отдельно взятый индивид оказывается в центре коммуникативного пространства, основанного на глобальном взаимодействии, которое влияет на развитие идей, норм, ценностей, моделей поведения. Государственные институты сталкиваются со все более отчетливыми вызовами со стороны международной миграции, средств массовой информации и, конечно, сети интернет»[151].

Воздействие научно-технического прогресса в информационной сфере на процессы безопасности привело к возникновению такой новой области обеспечения национальной безопасности, как информационная безопасность.

---

[149] Закон Украины «О Совете национальной безопасности и обороны Украины» от 5 марта 1998 г. № 183/98-ВР // http://base.spinform.ru/show_doc.fwx?rgn=17928 (дата обращения: 18.12.2013)

[150] Об информатизации: Закон Республики Таджикистан 06.08.2001 г. № 40.

[151] Санина А. Г. Информационное общество и государственная идентичность // Информационное общество. 2013. № 6. С. 10.

Инновационные свойства коммуникативного пространства, позволяющего осуществлять взаимодействие субъектов информационных процессов одновременно на самых разных уровнях – от индивидуального до глобального, потребовало и комплексного подхода к обеспечению информационной безопасности. В этой сфере особенно явно проявляется зависимость поддержания национальной информационной безопасности от участия государства в обеспечении информационной безопасности на глобальном уровне и от защищенности безопасности индивидов в информационной сфере.[152]

Подобные инновационные и комплексные проблемы возникли и в целом ряде других ключевых областей жизнедеятельности мирового сообщества и ведущих государств. К таким областям следует отнести обеспечение экологической, климатической, энергетической, сырьевой безопасности и др.

Итак, глобальное развитие коренным образом преобразило сферу безопасности как на всемирном, так и на национальном уровнях, придав ей инновационный, комплексный и динамичный характеры. В данной связи потребовалось изменение системы национальной безопасности: сначала в наиболее развитых, а затем и во многих других государствах. Потребовалось качественно новая форма координации сил и средств, обеспечивающих безопасность на всех уровнях.

Роль такого координатора была возложена на Советы безопасности, как на важнейшие государственные органы, действующие на национальном уровне. Во многих странах этим советам придается чрезвычайно высокий статус, и они являются конституционными органами. Таким образом, произошли существенные системные изменения в обеспечении национальной безопасности, имеющие институционально-политическое измерение, и одновременно обусловленные действием научных и технологических факторов.

Следует отметить, что сложность задач в области обеспечения информационной безопасности в ближайшие годы и десятилетия будет только

---

[152] Конституция Исламской Республики Иран // http://read24.ru/fb2/konstitutsionnoe-sobranie-konstitutsiya-islamskoy-respubliki-iran/ (дата обращения: 25.10.2013)

нарастать. Так, по расчетам компании «Cisco», сейчас на каждого человека на Земле приходится два «умных» устройства, которые могут обмениваться информацией между собой: например, смартфон, навигатор и автомобиль с бортовым компьютером. По прогнозам, к 2020 году таких приборов на каждого человека будет в среднем семь[153].

Таким образом, возникает инновационная информационно-коммуникативная среда, в которой «умные приборы» будут общаться друг с другом, а также с интеллектуальными комплексными системами типа «умный дом» или «безопасный город» и тому подобное. Эти приборы будут контактировать через «Глобальную паутину», которая постепенно превратится в «Интернет вещей» и начнет существовать параллельно, а в определенных ситуациях – пересекаясь с «Интернетом людей».

Исследователь Е. Носов, оценивая развитие рассматриваемой ситуации, пишет: «Интернет вещей», по прогнозам, разовьется в полном масштабе уже через 10 лет. Мир изменится до неузнаваемости, станет удобным для человека. Правда, как отмечают специалисты, существует одна большая проблема – безопасность человека в техносреде. Еще никто не предложил решения, способного контролировать огромную бездушную сеть, от которой будет зависеть жизнь человека.

Чтобы представить степень угрозы в случае проникновения вируса, киберпреступников или просто сбоя программы, стоит только вспомнить сценарии большинства голливудских блокбастеров о восстании машин»[154].

Наряду с изменением институциональной составляющей, в XXI веке происходят и другие принципиальные изменения в системе обеспечения национальной безопасности. В этой системе важную роль играют силы и средства обеспечения ее информационной составляющей, как второго важного системообразующего сегмента.

---

[153] Носов Е. Власть вещей. Человечество стоит на пороге создания информационной среды, в которой гомо сапиенс будет лишним // Итоги. 2013. - №51(915).-С. 56.

[154] Там же.

В «Стратегии национальной безопасности Российской Федерации до 2020 года» дано следующее определение: «…«средства обеспечения национальной безопасности» – технологии, а также технические, программные, лингвистические, правовые, организационные средства, включая телекоммуникационные каналы, используемые в системе обеспечения национальной безопасности для сбора, формирования, обработки, передачи или приема информации о состоянии национальной безопасности и мерах по ее укреплению»[155].

В последнее время существенно возрастает роль информационных технологий в процессах обеспечения национальной безопасности, что ведет к принципиальным изменениям в ее системе. Эти технологии обеспечивают прием и передачу, обработку и накопление информации. Для реализации данных процессов используют соответствующие способы и приемы, средства и формы, которые составляют основу информационных технологий.

Современные информационно-коммуникационные технологии дают возможность хранить, передавать и обрабатывать информационные массивы в цифровом формате. В последние десятилетия данный формат позволил создать невиданные ранее возможности для передачи информации виде числовых сигналов, что позволило создать национальные, региональные и глобальные информационно-коммуникационные сети и в итоге – глобальное информационное пространство. Использование цифровых технологий позволило придать новый импульс освоению космического пространства.[156]

Таким образом, человеческая цивилизация в XXI веке все более и более зависит от развития информационно-коммуникационных технологий. Данная ситуация существенным образом влияет на процессы в сфере безопасности, в которых все большую роль начинают играть процессы обеспечения информационной безопасности.

---

[155] Стратегия национальной безопасности Российской Федерации до 2020 г. Утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537 // Российская газета. 2009. 19 мая. Гл. 1. Ст. 6.

[156] Использование информационно-коммуникационных технологий в целях развития: Резолюция Генеральной Ассамблеи ООН № A/RES/65/141 от 20 декабря 2010 года [Электронный ресурс]. – Режим доступа: http://daccess-dds-ny.un.org/ doc/UNDOC/GEN/N10/521/02/PDF/N1052102.pdf?OpenElement. (дата обращения: 19.02.2014)

Эксперты отмечают: «Само понятие информационной безопасности имеет два аспекта: с одной стороны, безопасность самих инфоресурсов – информации и технологий, к этой категории следует отнести вопросы обеспечения стабильного функционирования информационной инфраструктуры, защиты от несанкционированного доступа, вредоносных программ и пр. Этот аспект в основном носит технический характер, так как связан с умышленным или случайным воздействием на информацию или информационную инфраструктуру.

Другой, более широкий, включает, в первую очередь такие категории, как информационные ресурсы, обеспечивающие безопасность в целом, эффективность применения информационных технологий и пр.»[157].

Информационно-коммуникационные технологии используются практически во всех основных областях жизнедеятельности современного общества: как на национальном, так и на глобальном уровнях. В данной связи проблемы защиты информационных ресурсов в наши дни становятся все более острыми и злободневными.

Негативные воздействия на информационные ресурсы и потоки на информационную структуру в целом могут вызвать разрушительные последствия для областей человеческой жизнедеятельности, которые непосредственно не входят в информационную сферу, но в которых информационные ресурсы применяются для обеспечения их функционирования.

Такое положение дел позволяет сделать вывод о том, что в современных условиях информационная безопасность превратилась в системообразующий элемент всей структуры национальной безопасности. Все основные направления национальной безопасности либо связаны с такими областями общественной жизни, в которых информационно-коммуникационные технологии играют важную роль, и их применение требует самой тщательной защиты, либо в процессе обеспечения национальной безопасности по всем основным направлениям широко применяются указанные технологии, и их несовершенство,

[157] Шариков П. А. Эволюция государственной стратегии в сфере информационной безопасности // США – Канада: Экономика, политика, культура. 2009. Декабрь. № 12. С. 95.

неэффективность применения (или отставание от передовых мировых образцов) может привести к затруднениям (или нарушениям в защите национальной безопасности).

Итак, можно констатировать, что в наши дни произошла информатизация всей системы национальной безопасности. Рассматриваемый процесс не только предполагает применение информационно-коммуникационных технологий для технического обеспечения национальной безопасности, но с их помощью принимаются принципиальные решения тактического и стратегического характера для реализации процессов в указанной области. И, наконец, сами информационные технологии требуют зашиты и охраны во всем спектре своего применения, который продолжает расширяться, что открывает новые возможности для дальнейшего развития и преобразования всей системы национальной безопасности.

Информационно-коммуникационные технологии в наше время используются как по отдельности, так и системно – в различных конфигурациях. Наиболее распространенной формой применения стали компьютерные сети. Эти сети могут иметь масштабы от локальных сетей (в рамках одной организации, одного дома) до глобальных сетей: например, Internet, GPS, GLONASS и так далее.

Таким образом, в последнее время на основе информационных технологий возникла новая сфера общественной жизнедеятельности – сфера сетевых коммуникаций, которая стала основой для инновационной социальной структуры современного общества. Сетевые информационно-коммуникационные структуры существенно повлияли на временные и пространственные характеристики современного мира международного сообщества, а также национальных и местных сообществ.

Информационные потоки распространяются в наши дни с очень высокой скоростью, а объемы передаваемой информации стали представлять огромные массивы текстовой, аудио-, видео- и иной информации. Подобная ситуация была практически недоступна еще несколько десятилетий назад.

Жизнедеятельность современного мира осуществляется в едином, глобальном информационном поле, которое образовано совокупностью множества сетевых коммуникаций. Однако, наряду с несомненными и очевидными преимуществами для развития современной цивилизации такой сетевой коммуникационной мегаструктуры, она несет в себе как очевидные, так и скрытые угрозы национальной безопасности.

Так, Т. В. Владимирова отмечает: «В современном обществе все большее количество коммуникаций принимает сетевой характер. Разрастание таких структур сопровождается увеличением интенсивности коммуникаций и становится причиной многих серьезных проблем, связанных с безопасностью личности, общества и государства. По сути, речь идет о росте дифференциации социальных процессов, и, соответственно, их усложнении и ускорении. Подобная ситуация требует изучения сетевого коммуникативного пространства»[158].

Таким образом, в наше время, человечество столкнулось с созданием в дополнение к миру людей, который существует испокон веков в физическом пространстве, мира, который возник и развивается в виртуальном пространстве. Это пространство, как известно, создано с помощью информационно-коммуникационных технологий. В начале становления данных технологий и широкого их внедрения в жизнь общества возникло понятие информационной безопасности, которое трактовалось в основном под техническим и правовым углами зрения.

С данным видом безопасности связывали, в первую очередь, вопросы защиты конфиденциальности, обеспечения достоверности и полноты информации, адекватности методов обработки информации, доступность информационных ресурсов, а также защиту программного обеспечения и коммуникационных линий и магистралей.

Однако, в современных условиях информационная безопасность сопряжена не только с техническим и правовым обеспечением устойчивого

[158] Владимирова Т. В. Сетевые коммуникации как источник информационных угроз // Социологические исследования. 2011. № 5. С. 123.

функционирования информационно-коммуникативных сетей. Информационная безопасность сегодня включает в себя обеспечение защиты личности, общества и государства в новой социальной реальности, существующей в виртуальном пространстве и неразрывно связанной с традиционным обществом реального мира.

При таком подходе к пониманию информационной безопасности объем и рамки этого феномена существенно расширяются. В поле обеспечения информационной безопасности включаются не только вопросы технического и правового характера, но и жизненно важные проблемы, имеющие политическую, социальную, экономическую и психологическую природу (Рисунок 3).

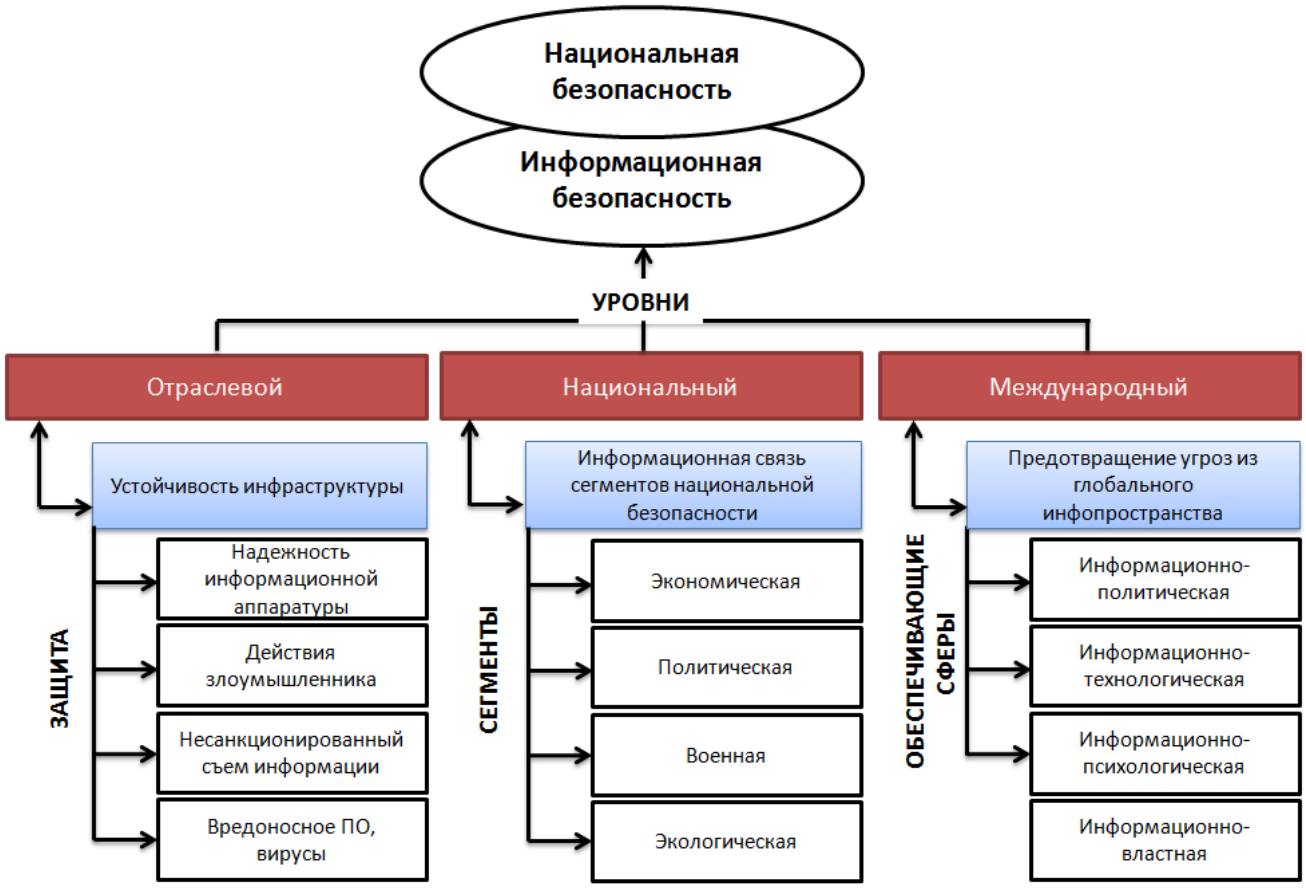


Рисунок 3 – Уровни обеспечения информационной безопасности

Кроме того, информационная безопасность в наши дни оказывается непосредственно сопряженной с кругом задач, которые входят, в качестве приоритетных, в состав проблемного поля национальной безопасности в целом и

направлены на обеспечение нормальной жизнедеятельности личности, общества и государства.

Российские исследователи активно обсуждают угрозы и опасности, которые возникают в современном информационном пространстве и имеют важное социально-политическое значение, далеко выходящие за рамки обеспечения технической безопасности и которые можно реально отнести к сфере обеспечения национальной безопасности.

Например, уже упомянутая Т. В. Владимирова выделяет основные группы информационных угроз безопасности личности, общества, государства, обусловленных сетевыми коммуникациями:

«– Угрозы безопасности личности, связанные с расширением возможностей манипулирования сознанием человека, информационной перегрузкой, с ростом Интернет-зависимости и развитием форм психосоциальной депривации.

К этой же группе отнесем угрозы использования во вред персональных данных (расширение возможностей скрытого сбора персональной информации);

– Информационные угрозы, связанные с расширением масштабов манипуляции общественным мнением, появлением возможностей эффективной организации деструктивных процессов в ценностных системах общества;

– Угрозы безопасности личности, общества, государства, связанные с работой сетевых структур отечественной и международной преступности и терроризма;

– Угрозы стабильности существующих политических режимов власти: системные и периферийные, также обусловленные сетевой логикой многих социальных процессов в обществе»[159].

Таким образом, следует отметить, что под воздействием стремительного развития информационно-коммуникационных технологий информационная безопасность выступает в качестве одного из ведущих факторов системных изменений в структуре и содержании национальной безопасности в целом.

[159] Там же. С. 127.

На международном уровне процессы обеспечения информационной безопасности в мировом сообществе заняли центральное место в деятельности человеческого сообщества по поддержанию международной безопасности. Так, в разработанной Российской Федерацией концепции «Конвенции об обеспечении международной информационной безопасности» уже в преамбуле придается «важное значение международной информационной безопасности как одному из ключевых элементов системы международной безопасности»[160].

Подобное понимание роли фактора информационной безопасности в развитии системы безопасности на национальном и международном уровнях сложилось в политической мысли и правовом сознании ведущих стран современного мира, что нашло отражение в официальных государственных документах.

Первыми за рубежом об информационной безопасности заговорили в США. Руководство Соединенных Штатов считает, что информационные потоки и ресурсы представляют собой фактор стратегического характера, если для их обработки применять новейшие информационные технологии.

Во-первых, использование данных технологий позволяет получить значительно больше сведений о противнике, повысить осведомленность о его военных возможностях. С помощью информационно-коммуникационных технологий, можно воздействовать на противника, используя методы ведения информационной войны и значительно затруднять оборонительные действия противоположной стороны.

Во-вторых, применение современных информационных технологий позволяет сделать более эффективным взаимодействие между различными родами войск и конкретными подразделениями, прежде всего, на командном уровне, включая органы боевого управления и разведки. Такой подход, по мнению американских экспертов, позволит реализовать информационное превосходство США в кризисных ситуациях по всему миру.

---

[160] Конвенция об обеспечении международной информационной безопасности (концепция) // http://www.scrf.gov.ru/documents/6/112.html (дата обращения: 18.01.2014)

После своего избрания президент Б. Обама был ознакомлен с докладом Управления национальной разведки США «Глобальные перспективы – 2025», в котором содержится заключение о «назревшей необходимости принятия мер противодействия информационным угрозам», а также о том, что эти угрозы должны рассматриваться на уровне национальной безопасности страны.

К аналогичному выводу пришли авторы другого доклада, подготовленного в Центре стратегических и международных исследований и непосредственно посвященного политике кибербезопасности, проводимой Белым домом в настоящее время. В нем президенту Б. Обаме рекомендуется принять неотложные меры с тем, чтобы не допустить по этому направлению обострения угрозы национальной безопасности[161].

Первостепенное внимание проблемам информационной безопасности уделяет руководство Китая. В КНР информационные угрозы относят к нетрадиционным угрозам национальной безопасности. Под традиционными угрозами китайские эксперты понимают локальные войны и вооруженные конфликты, наращивание вооруженных сил крупными мировыми державами, а также проблемы нераспространения ядерного оружия.

Однако, китайские аналитики отмечают влияние информационного фактора и на эволюцию традиционных угроз национальной безопасности в условиях современного глобального развития. Так, директор Китайского института международных стратегических исследований Сюн Гуанкай пишет: «…крупные мировые державы постоянно наращивают военные расходы для трансформации своих вооруженных сил, ядром которой служат информационные технологии»[162].

Китайские эксперты разделяют угрозы безопасности, существующие в современном мире, на традиционные и нетрадиционные. Традиционные угрозы, по их мнению, проявляются, прежде всего, в политической и военной сферах. К таким угрозам китайские специалисты в области безопасности относят гегемонизм и политику с позиции силы. Данные традиционные угрозы

[161] Пашков В. Информационная безопасность США // Зарубежное военное обозрение. № 10. 2010. С. 7.
[162] Сюн Гуанкай. Всеобъемлющая концепция национальной безопасности Китая // Россия в глобальной политике. 2010. Т. 7. № 3. С. 93.

проявляются в следующем: рост числа локальных войн и вооруженных конфликтов, наращивание военных расходов и вопрос о нераспространении ядерного оружия.

Нетрадиционные угрозы, как полагают аналитики из Китайской Народной Республики, трансформируются в весомый фактор, негативно воздействующий на глобальную безопасность. Центральной проблемой среди нетрадиционных угроз является опасность терроризма. Кроме того, к этому типу угроз относят также острые проблемы в таких областях, как финансы, энергетика, продовольствие, изменение климата, информационная безопасность, безопасность пищевых продуктов и здравоохранение. Информационная безопасность считается одной из важнейших среди указанных проблем.

Сюн Гуанкай следующим образом формулирует новую концепцию Китая в сфере обеспечения международной безопасности: «В области международного сотрудничества по безопасности мы выступаем за реализацию новой концепции, которая гласит: «Взаимное доверие, взаимовыгода, равноправие, взаимодействие».

Это идентично основным целям и принципам ШОС – шанхайскому духу, характеризующемуся как «взаимное доверие, взаимовыгода, равноправие, взаимодействие, уважение многообразия цивилизаций и стремление к совместному развитию». КНР и РФ – инициаторы создания ШОС и основные творцы шанхайского духа»[163].

Российские исследователи обращают внимание на стремление властей КНР расширить возможность контроля за информационным пространством. Для этих целей китайские военные стремятся получить доступ к новейшим информационно-коммуникационным технологиям. Такой подход рассматривается как важнейшее направление деятельности с целью ослабить зависимое положение в информационно-технологической сфере от ведущих стран Северной Америки и Западной Европы.

---

[163] Там же. С. 98.

Так, консультант ПИР-Центра Г. Р. Ибрагимова отмечает: «Для расширения возможностей Китая в киберпространстве НОАК активно взаимодействует с коммерческими организациями и сферой образования, что способствует получению доступа к передовым исследованиям и технологиям, в том числе к телекоммуникационным системам военного и двойного назначения. Снижение зависимости от информационно-коммуникационных технологий Запада и развитие собственного инновационного потенциала рассматриваются как важные средства обеспечения кибербезопасности КНР»[164].

Российская Федерация и Китайская Народная Республика имеют благоприятные возможности для сотрудничества в области обеспечения информационной безопасности как в двухстороннем формате, так и в рамках международных организаций. Наиболее перспективной для такого сотрудничества представляется Группа БРИКС. Российское информационное пространство является самым большим в Европе, а китайский сегмент Интернета – крупнейшим в мире.

Кроме того, страны БРИКС находятся в важнейших частях света, определяющих глобальное развитие: в Европе, Азии, Америке и в Африке. Число пользователей Всемирной паутиной в этих странах составляет половину мировой интернет-аудитории.

Российские аналитики полагают, что в формате БРИКС наша страна и ее партнеры могли бы искать пути решения следующих проблем:

− ограниченность и нехватка эффективных механизмов борьбы с трансграничной киберпреступностью;

− глобальное цифровое неравенство, выражающееся в неравномерности развития интернет-инфраструктуры в современном мире;

− подготовка концептуального документа по обеспечению глобальной информационной безопасности и последующее продвижение его в международных организациях;

---

[164] Ибрагимова Г. Р. Стратегия в области управления Интернетом и обеспечения информационной безопасности // Индекс безопасности. 2013. Т. 19. № 1 (104). С. 181.

− усиление мер доверия и обмена информацией в области кибербезопасности и тому подобное.

«В интересах как БРИКС в целом, так и России в частности – реализация совместных проектов развития трансконтинентальной ИКТ-инфраструктуры (оптоволоконные кабели и тому подобное) с целью повышения устойчивости и надежности телекоммуникаций между странами БРИКС и расширения доступа населения стран группы к широкополосному доступу в Интернет. В этот контекст хорошо вписывается обсуждаемый сегодня проект трансконтинентального подводного интернет-кабеля, который соединил бы все страны БРИКС, расположенные на трех континентах, напрямую»[165].

Государства БРИКС имеют примерно равные позиции в мировом информационном пространстве и могли бы успешно сотрудничать в обеспечении информационной безопасности в условиях системных изменений в сфере национальной и международной безопасности.

2.2. Политика модернизации национальной безопасности Российской Федерации в условиях глобального информационного общества

Во второй половине XX века сформировались предпосылки и начался переход к глобальному информационному обществу**.** Американский теоретик Д. Белл выпустил (1973 г.) книгу «Грядущее постиндустриальное общество. Опыт социального прогнозирования»[166]. Согласно выводам и прогнозам создателя концепции постиндустриального общества, такая социальная формация обладала следующими отличительными чертами:

− превращение сферы услуг в ведущий сектор экономики;

− становление знаний в качестве основной силы общественного развития;

[165] Баклицкий А., Бужинский Е., Демидов О., Лузин П., Орлов В. БРИКС и передовые технологии: перспективы сотрудничества и интересы России // Индекс безопасности. 2013. Т. 19. № 4 (107). С. 86.
[166] Bell D. The coming of post-industrial society. A venture of social forecasting. N.Y.: Basic Books, 1973.

− преобладание в структуре занятости населения представителей новой интеллектуальной технологии – носителей знаний (ученых, профессиональных администраторов, инженеров, научных сотрудников и тому подобное);

− ведущая роль технологий и технологических оценок в развитии общества, применение «интеллектуальных технологий» в принятии решений.

Идеи Д. Белла получили развитие в работах многих теоретиков. Одну из наиболее заметных концепций, оказавших существенное влияние на общественное сознание, выдвинул О. Тоффлер в своей работе «Третья волна»[167]. «Третьей волной» он назвал наступление нового основного этапа в развитии цивилизации.

«Первая волна» возникла 10 000 лет назад и была связана с внедрением сельского хозяйства в жизнь людей, что привело к созданию аграрного (доиндустриального) общества. «Вторая волна» перемен, связанная с промышленной революцией, началась в XVIII веке и привела к переходу человечества к индустриальному обществу. В середине XX века зародилась «третья волна» в развитии цивилизации, которая привела к новому этапу социального развития. Этот этап в работах исследователей второй половины прошлого столетия назывался по-разному: постиндустриальное общество, супериндустриальное общество, технотронное общество и тому подобное.

Изучению данного феномена глобального развития посвятили свои работы многие ведущие западные исследователи: Г. М. Маклюэн, М. Кастельс, П. Друкер, Е. Масуда и др[168]. Советские ученые Э. А. Араб-Оглы, И. В. Бестужев-Лада, В. В. Загладин, И. Т. Фролов и др.[169] в это же время обсуждали наступление

---

[168] Маклюэн М. Галактика Гутенберга. Становление человека печатающего. М.: Академический проект, 2005. 496 с.; его же, Понимание медиа: внешние расширения человека М.: Кучково поле, 2007. 464 с.; Друкер П. Менеджмент. Вызовы XXI в. М.: Манн, Иванов и Фербер, 2012. 256 с.; Masuda Y. The Information Society as Postindustrial Society. Wash.: World Future Soc., 1983. 299 p.

[169] Араб-Оглы Э. А. Обозримое будущее. Социальные последствия НТР: год 2000. М.: Мысль, 1986. 205 с.; Бестужев-Лада И. В. Нормативное социальное прогнозирование. Возможные пути реализации целей общества. М.: Наука, 1987. 214 с.; его же, Поисковое социальное прогнозирование: перспективные проблемы общества. М.: Наука, 1984. 71 с.; Загладин В. В., Фролов И. Т. Глобальные проблемы современности: научный и социальный аспекты. М.: Международные отношения, 1981. 240 с.

научно-технической революции (НТР) и высказывали схожие идеи о возрастании роли технологического фактора в общественном развитии.

Впервые, в достаточно отчетливом виде идея информационного общества была сформулирована в конце 60-х – начале 70-х годов XX столетия. Изобретение самого термина «информационное общество» приписывается профессору Токийского технологического института Ю. Хаяши.

Контуры информационного общества были обрисованы в отчетах, представленных японскому правительству рядом организаций: Агентством экономического планирования (EPA: Economic Planning Agency) – «Японское информационное общество: темы и подходы»; Институтом разработки использования компьютеров (JACUDI: Japan Computer Usage Development Institute) – «План информационного общества»; Совета по структуре промышленности (ISC: Industrial Structure Council) – «Контуры политики содействия информатизации японского общества»[170].

Японские исследователи понимали информационное общество как такую социальную систему, где широкое распространение компьютерных технологий качественно изменит характер работы с источниками информации и информационными потоками. Прежде всего, они вели речь об изменении характера производства, которое, по их мнению, должно было стать высоко автоматизированным, а продукты такого производства – гораздо более информационно-емкими.

Наступление информационного общества, по мнению создателей этой концепции, могло иметь не только экономические, но социальные, а также политические последствия. Люди освобождались от монотонного, однообразного труда, получали более широкие возможности для творчества. Кроме того, предполагалась, что в информационном обществе исчезнут социальные классы и конфликты. В нем будет достигнуто общественное согласие и социальный мир.

[170] Подробнее см.: Алексеева И. Ю. Возникновение идеологии информационного общества // Информационное общество. 1999. Вып. 1. С. 30

Значительно уменьшится государственный аппарат по сравнению с предыдущими этапами исторического развития, правительства будут компактными и эффективными. В отличие от индустриального общества, ориентированного на потребление как на главную жизненную ценность, в информационном обществе главной ценностью станет время, произойдет увеличение значения бюджета свободного времени, которое можно будет посвящать культурному досугу и саморазвитию.

Таким образом, современные представления об информационном обществе нашего времени сформировались благодаря конвергенции трех концепций общественного развития, сформировавшихся во второй половине XX века. К ним следует отнести получившие широкое распространение в академическом сообществе, элитарном и массовом сознаниях следующие теоретические построения:

- теорию постиндустриального общества (postindustrial society);
- собственно концепцию информационного общества (information society);
- концепцию сетевого общества или социальных сетей (network society).

Теория постиндустриального общества возникла в условиях глобальной политической конфронтации, вызванной «холодной войной», финансово-экономических и энергетических кризисов 1960-1970-х годов. Авторы данной теории рассматривали ее как футурологический проект, описывающий идеал будущего общественного развития. Постиндустриализм рассматривался как новая стадия общественного развития, которая приходит на смену индустриальному обществу.

В постиндустриальном обществе, по замыслу авторов концепции, должны были исчезнуть основные социально-экономические противоречия и проблемы, возникшие на предыдущих стадиях общественного развития. Таким образом, постиндустриальное общество представлялось гораздо более безопасным и комфортным для людей, которые могли бы жить в нем, чем все предыдущие социальные системы. В данной связи изучению вопросов обеспечения безопасности в постиндустриальном обществе не уделялось значительное

внимание. Эти вопросы если и рассматривались, то только в связи с гораздо более общими проблемами социального развития.

Авторы концепции постиндустриального общества, создавая новый общественный идеал, делали акцент, прежде всего, на преимуществах и достоинствах этой социальной системы. В качестве основных отличительных черт такого общества выделялись следующие:

- ведущая роль инновационного сектора в экономике;
- преобладание высокопроизводительной промышленности;
- превращение знаний в главную производительную силу, создание индустрии знаний;
- превращение сферы услуг в ведущую область общественного производства, выход процесса оказания услуг на качественно новый уровень, когда они становятся многообразными, высококачественными и охватывают все стороны человеческой жизнедеятельности.

Однако, наступавшее постиндустриальное общество, по мнению создателей этой концепции, не является свободным от опасностей и рисков. В этом обществе также существует потребность обеспечения безопасности, и возможно, даже в большей степени, чем в предшествующем ему индустриальном обществе.

Вот, что пишет по этому поводу немецкий политический философ и социолог Ульрих Бек в статье «От индустриального общества к обществу риска»: «В абсолютной безопасности нам, людям, явно отказано. Но, скорее всего, неизбежный «остаточный риск» – это оборотная сторона беспрецедентных благоприятных возможностей (процветания, относительно высокого уровня социального обеспечения и общего комфорта), предлагаемых развитым индустриальным обществом большинству своих членов»[171].

Новые угрозы для постиндустриального общества имеют природу, связанную с научно-техническим прогрессом и с политико-правовой сферой. Кризис политических и административных институтов в конце XX в., контексте нового технологического прорыва, ведущего к созданию инновационных

[171] Beck U. From Industrial Society to the Risk Society // Theory, Culture and Society, February 1992. V. 9. No. 1. P. 98.

отраслей промышленности и новых видов вооружений. Особое вынимание теоретики постиндустриализма обращали на ядерные и химические, экологические и генетические технологии, развитие которых проходили в условиях ослабления систем, обеспечивающих политическую безопасность. Это ослабление имело причины, связанные как с дисфункциями административной системы, так и со сменой мировоззренческих установок.

У. Бек отмечает: «Главный социально-исторический и политический потенциал экологических, ядерных, химических и генетических опасностей кроется в крушении административной системы, в крахе научно-технической и правовой рациональности, а также институциональных гарантий политической безопасности, потребность в которых становится настоятельной необходимостью для каждого»[172].

Однако, дальнейшее общественное развитие показало, что ядром, системообразующим элементом постиндустриального общества стала его информационная сфера. Информационно-коммуникационные технологии вошли практически во все основные отрасли народного хозяйства и сферы общественной жизни. Кроме того, на их основе было создано, параллельное социальному пространству, виртуальное пространство, которое в итоге расширилось до глобального пространства, на базе которого возникло глобальное информационное общество. По этой причине постиндустриальное общество все чаще стали отождествлять с информационным обществом.

Возникшую несколько десятилетий назад теорию информационного общества следует, в определенной мере, рассматривать как конкретизацию и привязку к реалиям глобального развития концептуальных положений доктрины постиндустриального общества.

Одними из первых обратили на это внимание авторы десятого доклада Рисскому клубу «Микроэлектроника и общество. На радость или на горе», который был достаточно популярен в первой половине 1980-х гг. и оказал определенное влияние на формирование концепции информационного общества.

---

[172] Ibid. P. 123.

В данном исследовании сделан следующий вывод: «Микроэлектроника посредством миниатюризации, автоматизации, компьютеризации и роботизации, фундаментальным образом трансформирует нашу жизнь и преобразует большинство ее сторон, связанных с работой, бытом, политикой, наукой, военной деятельностью и поддержанием мира»[173].

В информационном обществе центральное место в системе безопасности, на современном этапе социального развития, стала занимать информационная безопасность. Некоторые аналитики пытались осмыслить данный феномен и уже на стадии разработки концепции информационного общества предупреждали, что не следует испытывать эйфорию от быстро развивающихся информационно-коммуникационных технологий.

Наряду с колоссальным вкладом в процесс развития общества и цивилизации, они создавали и новые проблемы, и прежде всего в сфере безопасности. Так, А. Кинг, один из соавторов работы ««Микроэлектроника и общество. На радость или на горе» в начале 80-х годов прошлого столетия выделял следующие основные тенденции влияния прогресса информационно-коммуникационных технологий на эволюцию общества:

− возрастание огромной взаимозависимости индивидов и наций благодаря мгновенному доступу к информации;

− создание возможностей для достижения высокого уровня децентрализации власти и процесса принятия решений, что было бы весьма желательно, но равным образом эти возможности могут быть использованы недобросовестными руководителями для усиления и консолидации централизации власти;

− возникновение контроля всех видов деятельности со стороны диктаторов и тоталитарных обществ по типу оруэлловского «Большого брата»;

− усиление уязвимости и хрупкости общества благодаря созданию огромных электронных баз данных, содержащих громадные массивы данных,

[173] Microelectronics and Society: For Better or For Worse. A Report to the Club of Rome / Ed. by G. FRriedrichs and A. Shaff. – Oxford etc.: Pergamon Press, 1982. P. V.

имеющих важное значение для общественной и личной жизнедеятельности, и к которым можно получить доступ, находясь даже на огромном расстоянии от этих баз;

− возрастающая зависимость жизнеобеспечивающих систем больших городов и государств в целом от применяемых для их обеспечения и функционирования информационно-коммуникационных систем;

− генерирование информационным обществом культуры поведения людей, основанной на самоизоляции и отчуждении от реального мира путем ухода в виртуальное пространство[174].

Особо следует рассмотреть концепцию «сетевого общества» и ее роль в формирование представлений о безопасности в условиях информационного общества. Данная концепция в целом сформировалась к концу прошлого XX столетия. Наиболее важный вклад в ее формирование внесли М. Кастельс, Я ван Дейк, Б. Веллмен и др. Важнейшими характеристиками сетевого общества необходимо рассматривать следующие его черты:

− возрастание роли в жизнедеятельности людей сетевых структур, которые постепенно заменяют формы личных и вещественных отношений, сложившиеся на предыдущих этапах социальной эволюции;

− сетевое общество представляет собой социальную структуру информационной эры, в которой экономические, политические и другие жизненно важные сети образуют виртуальное пространство, представляющее собой новую форму общественного взаимодействия;

− динамичный характер развития сетевого общества, представляющего собой открытую систему, восприимчивую к инновациям, которые осуществляются органично без размывания основ этой социальной структуры.

Российские исследователи полагают, что концепция социальных сетей дает возможность ученым применить новые подходы к исследованию общественного развития. В фокусе таких подходов оказываются социальные коммуникации и социальные контакты.

---

[174] Ibid. P. 27–29.

А. В. Назарчук отмечает: «Теория сетей определяет понимание социальности, трактуя социальный контакт как бинарную коммуникацию, коммуникацию между передающей и принимающей сторонами. Тем самым базовые понятия социальной теории коммуникативно операционализируются, то есть интерпретируются в ключе коммуникативных событий. Каждое социальное явление трактуется как совокупность «сообщений», способных транслироваться, накапливаться, виртуализироваться и так далее.

Этот атом, к которому может быть сведено все многообразие социальной реальности, можно назвать термином «сообщение» – massage. В сетевом обществе все становится «сообщением» или потоком «сообщений»: наполнение личной жизни, политические события, явления культуры и так далее»[175].

Таким образом, обеспечение безопасности потока сообщений в сетевом обществе превращается в базовую задачу обеспечения безопасности всей социальной системы, существующей в информационную эпоху.

В условиях современной России, перешедшей на информационную стадию развития, обеспечение информационной безопасности имеет принципиальное значение для успешного функционирования всей системы национальной безопасности. Для этого требуется реализация последовательной политики модернизации системы национальной безопасности нашей страны. Такой подход определяется группой принципиально важных факторов.

Информационно-коммуникационные технологии развиваются очень динамично, что приводит не только к потребности постоянного внедрения новых технических решений, но и ведет к серьезным изменениям в различных жизненно важных сферах общества: социальной, политической, духовной, экономической и других областях.

Наглядным примером может служить Интернет – всемирная система компьютерных сетей, целью которой является хранение и передача информации. За несколько десятилетий Интернет прошел четыре важных этапа в своем

[175] Назарчук А. В. Сетевое общество и его философское осмысление // Вопросы философии. 2008. № 7. С. 70.

развитии. При этом каждый новый принципиально отличался от предыдущего этапа. Рассмотрим эти этапы более подробно:

1) первый этап, «исследовательский», продолжался с момента возникновения вплоть до 1980-х годов – когда Интернет использовался, главным образом, университетами (в научных целях);

2) «информационный» – второй этап: когда каждая компания стремилась вывести информацию о себе в Интернет, создать корпоративный сайт;

3) третий этап представлял собой переход от статичных данных к возможности совершать транзакции; не только читать о продуктах и услугах, но и покупать или продавать их;

4) «социальный», или Web 2.0, – четвертый этап: когда в Интернете популярность обрели социальные сети, которые позволяют пользователям связываться друг с другом, подключаться к указанным сетям и обмениваться персональной информацией. Причем пользователи становятся активными создателями контента и могут составить конкуренцию крупным медийным корпорациям[176].

Анализ основных этапов развития Интернета показывает, что за достаточно короткий, по историческим меркам, срок исследовательский проект, имевший научные цели превратился в базовую инфраструктуру, на основе которой создается глобальное информационное общество. Интернет и другие информационно-коммуникационные системы реально воздействуют на все основные сферы жизнедеятельности общества: политическую, экономическую, социальную, духовную, военную и др.

В данной связи следует обратить особое внимание на то, что информационно-коммуникационные технологии непосредственно влияют и на обеспечение национальной безопасности во всех вышеуказанных сферах общественной жизни.

---

[176] См.: Зиновьева Е. С. Международно-политические аспекты развития Интернета // Вестник МГИМО-Университета. 2013. № 4. С. 137–138.

Таким образом, при проведении политики дальнейшей модернизации системы национальной безопасности должен быть заложен принцип информационной достаточности для обеспечения национальной безопасности Российской Федерации как в целом – на уровне обеспечения национальной безопасности всей страны, так и на уровне отдельных жизненно важных сфер общественной жизни и конкретных регионов.

Информационная достаточность обеспечения национальной безопасности означает следующее:

- превращение информационной безопасности в системообразующий элемент всей системы обеспечения национальной безопасности России;
- обеспечение на мировом уровне современными инновационными информационно-коммуникационными технологиями всех важнейших социальных институтов и систем жизнеобеспечения российского общества;
- достижение эффективной защищенности всех информационных ресурсов и коммуникаций, используемых российским государством и обществом, а также гражданами нашей страны.

При реализации принципа информационной достаточности в политике модернизации национальной безопасности Российской Федерации следует учитывать сложный и комплексный характер этого понятия. Оно непосредственно связано с современной информационной средой, которая представляет собой сложное образование, состоящее из многих элементов – различных информационных пространств.

Данное обстоятельство следует самым непосредственным образом учитывать при реализации принципа информационной достаточности в процессе модернизации системы информационной и национальной безопасности.

А.А. Марков, обсуждая данную проблему, пишет: «На сегодняшний день, выработаны основные черты понятия информационной безопасности, предусматривающие, что в современном социуме информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и тому подобное) и информационно-

психологическую (естественный мир живой природы, включающий и самого человека).

Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической безопасностью»[177].

В отечественной научной литературе встречаются и другие подходы к определению основных элементов информационной безопасности. Они не содержат принципиальных отличий, но дают несколько иные дефиниции элементов данного вида безопасности или угроз, которые эти элементы формируют. Политолог В. П. Хрыков подчеркивает: «Условно опасности информационного общества можно разделить на информационно-технологические и коммуникационно-медийные»[178].

Деление информационной безопасности или угроз, определяющих ее содержание, на две составные части, приведенные выше, следует дополнить третьим элементом – информационно-политической безопасностью.

В современных условиях наблюдается интеграция политической и информационной сфер общественной жизни. Во-первых, в современных условиях постоянно возрастает роль информационного фактора в политике. Традиционные печатные и электронные средства массовой информации (СМИ) оказывают значительное влияние на массовое политическое сознание и даже на взгляды политических элит. Таким образом, СМИ оказывают непосредственное влияние на принятие важных политических решений, воздействуют на ход политических процессов как на национальном, так и глобальном уровнях, влияют на функционирование базовых политических институтов.

Во-вторых, в последние годы стремительно возрастает воздействие Интернета посредством социальных сетей и других информационно-

---

[177] Марков А. А. Характеристики информационной безопасности на современном этапе развития общества // Управленческое консультирование. 2011. № 3. С. 70–71.

[178] Хрыков В. П. Информационное общество в России: условия и проблемы формирования // Политика и общество. 2011. № 6. С. 20.

коммуникативных структур Всемирной паутины на политическое развитие общества.

Функционирование указанных инновационных информационных систем носит интерактивный характер. Оно происходит в аудиториях пользователей, которые составляют сотни миллионов человек, что позволяет решать не только задачи политического информирования и влияния на формирование политического сознания, но и выполнять политико-организационные и политико-мобилизационные функции.

«Современные процессы информатизации общества приводят к изменению структуры и технологии власти, – отмечает И. В. Сурма, – перераспределения влияния в пользу тех, кто управляет информационными потоками и ресурсами. «Информационный пресс» приобретает в современных международных отношениях приоритетное значение, что дает все основания отнести информацию к разряду факторов, определяющих коренные социальные перемены в современном мире»[179].

В-третьих, в современном глобальном информационном обществе стремятся доминировать США и поддерживающие их развитые западные страны. Такая ситуация ведет к утрате сбалансированности и устойчивости развития информационного общества.

В современных условиях политика модернизации системы национальной безопасности Российской Федерации в контексте глобального информационного общества должна строиться на использовании средств и сил обеспечения информационной безопасности в качестве системоообразующего фактора данного процесса и всей указанной системы в целом. Политику модернизации следует осуществлять по трем основным направлениям:

1) информационно-технологическое;
2) информационно-психологическое (коммуникационно-медийное);
3) информационно-политическое.

---

[179] Сурма И. В. Глобальный наднациональный актор международных отношений и его социальная философия // Вестник МГИМО-Университета. 2013. № 4. С. 142..

Рассмотрим более подробно данные направления. Первое – информационно-технологическое – связано с защитой технических и технологических составляющих российского информационного общества в аспекте обеспечения национальной безопасности нашей страны. Основные задачи, связанные с данным направлением деятельности, изложены в «Положении о Федеральной службе по техническому и экспортному контролю». К этим задачам, в том числе, относятся:

– реализация, в пределах своей компетенции, государственной политики в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации;

– осуществление государственной научно-технической политики в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

– организация деятельности государственной системы противодействия техническим разведкам и технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной государственной системой[180].

Процесс реализации данных задач требует их постоянной адаптации к меняющимся условиям современного глобального общества. Для этого необходим непрерывный учет инноваций в сфере развития информационно-коммуникационных технологий, совершенствования методов работы разведывательных служб зарубежных государств, активности негосударственных информационных структур и отдельных хакеров, стремящихся нанести ущерб национальной безопасности нашей страны.

Второе направление политика модернизации национальной безопасности Российской Федерации – информационно-психологическое или коммуникационно-медийное – имеет своей целью защиту общества, государства и

[180] Положение о Федеральной службе по техническому и экспортному контролю. Утверждено Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (редакция от 21.12.2013). // http://www.consultant.ru/document/cons_doc_LAW_156349/?frame=1 (дата обращения: 10.02.2014)

личности от неблагоприятного информационного воздействия на массовое или индивидуальное сознание. Причем следует отметить, что некоторые методы и приемы информационно-психологической борьбы ориентированы на воздействие не только на сознание, но и на подсознание людей.

Такое воздействие осуществляется в скрытой форме. Нужные противнику установки, стереотипы поведения и жизненные ориентиры внедряются в сознание и подсознание людей, «упакованными» в информационный контент, который, на первый взгляд, кажется достаточно безобидным.

В конечном счете, целями негативных информационно-психологических воздействий являются манипуляции общественным и индивидуальным сознанием. Данные манипуляции нацелены на изменение сознания в направлении, нужном для достижения политических (военных, экономических и других) целей, которые преследует сторона, организовавшая такое влияние. В ряде случаев такую деятельность представляет собой заранее спланированные и организованно проведенные интеллектуальные диверсии.

Данные манипуляции и диверсии осуществляются с помощью средств массовой информации, и в последние годы в эти процессы все активнее вовлекаются информационные ресурсы Интернета.

Третье направление политики модернизации национальной безопасности нашей страны – информационно-политическое. Разоблачения Э. Сноудена и других бывших сотрудников американских спецслужб показали, что Всемирная сеть используется и для сбора, зачастую путем кражи и несанкционированного доступа к информационным ресурсам, данных, имеющих откровенно разведывательный характер.

Причем такая деятельность осуществлялась американской стороной в огромных размерах, которые потрясли весь мир, включая и их западных союзников. В связи с этим федеральный канцлер Германии А. Меркель выдвинула идею о создании Европейской коммуникационной сети: для того чтобы избежать автоматического прохождения информационных потоков через американские информационные магистрали и серверы.

Российские эксперты по информационной безопасности подчеркивают: «Один из путей сохранить данные в тайне – это выпускать за пределы ЕС только нужную информацию. И персональные данные, и почта, и весь трафик не пересекут границ Евросоюза. Но и такая система, когда информация не идет через сети провайдеров США, не может исключить утечки данных, но уже по каналам разведки. Сейчас тренд на то, что Интернет не будет таким глобальным, каким он был до разоблачений Эдварда Сноудена»[181].

Акцент на деглобализацию Интернета означает, что другие крупные международные регионы (подобно Европейскому Союзу) и ведущие индустриально развитые государства (подобно Германии) начнут создавать собственные национальные и региональные информационно-коммуникационные сети. Такой подход позволит вывести Интернет из-под контроля правительства и разведывательных служб США. Однако, в данном случае Всемирная паутина распадется на ряд локальных сетей меньшего масштаба.

При модернизации системы обеспечения национальной безопасности России в условиях глобального информационного общества необходимо принимать во внимание три возможных сценария развития Интернета в среднесрочной перспективе (Рисунок 4).

[181] Шадрина Т. Невыносимая локальность сети // Российская газета. 2014. 18 февраля. № 37(6309). С. 1.

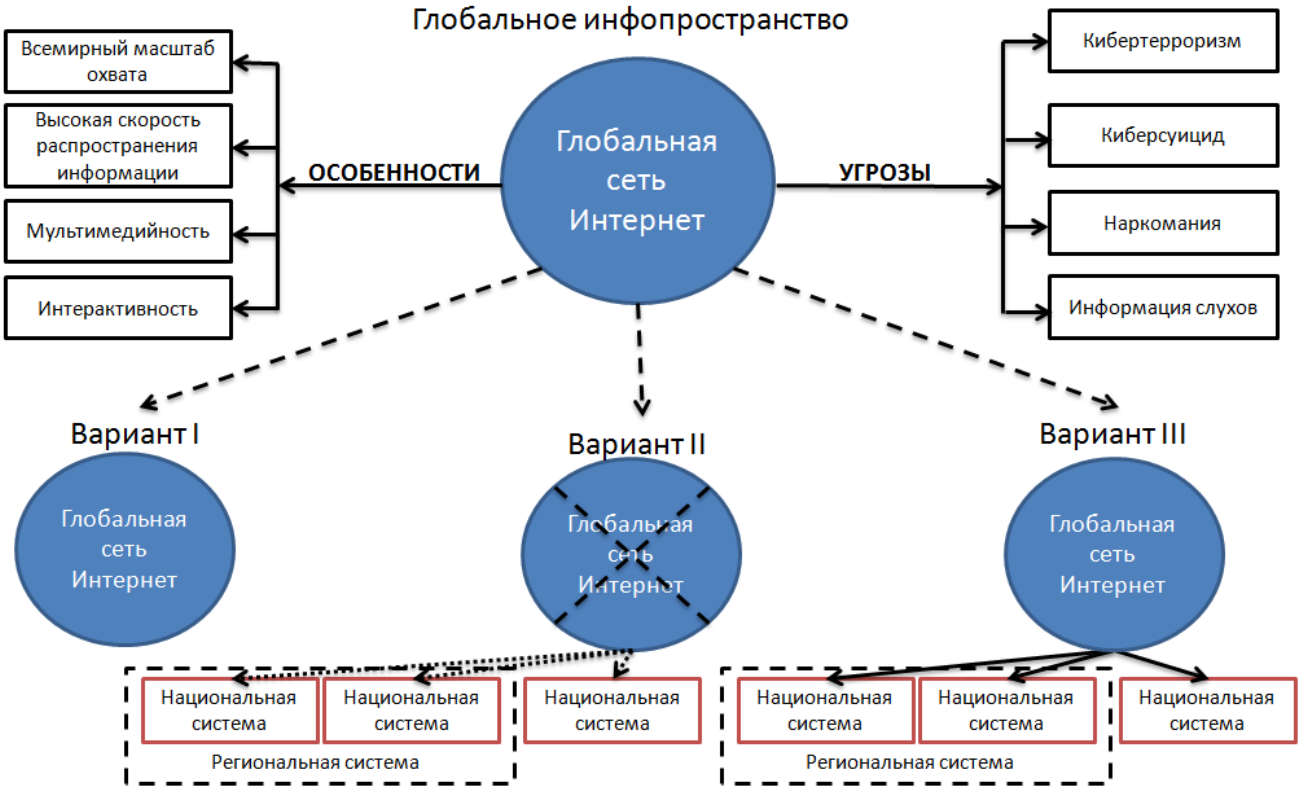


Рисунок 4 – Среднесрочный прогноз развития сети Интернет

Первый сценарий представляет собой такой путь дальнейшего развития Интернета, при котором в этой глобальной системе сохраняется сложившееся, на сегодняшний день, статус-кво с небольшими «косметическими» изменениями, направленными на то, чтобы пользователи во всем мире поскорее забыли громкий скандал, связанный с разоблачениями противоправной деятельности американских спецслужб.

Вероятность реализации такого сценария достаточно мала, так как меры по защите национальных сетей и более эффективному обеспечению национальной безопасности в информационном аспекте уже начали проводиться в ряде ведущих стран мира. Российская Федерация приступила к осуществлению таких мероприятий еще до вышеназванных разоблачений и скандалов.

Второй сценарий предполагает распад глобальной сети Интернет на региональные и национальные системы гораздо меньших масштабов, обособленные друг от друга различными защитными и контрольными

структурами. Таким образом, глобальная сеть превращается в совокупность локальных сетей.

Вероятность реализации такого прогноза в современных условиях также невелика. Она может существенно возрасти, если последуют новые разоблачения и вскроются новые кампании по глобальной слежке и проведению информационно-разведывательных мероприятий во всемирном масштабе.

Особо резкую негативную реакцию многих правительств суверенных государств может вызвать применение самых инновационных информационно-коммуникационных технологий нового поколения, открывающих принципиально иные возможности для осуществления глобального шпионажа.

Сценарий, который рассматриваемся в качестве третьего варианта возможного развития глобальной информационно-коммуникационной сети, является синтетическим и представляет собой сочетание первых двух рассмотренных выше прогнозов.

Данный сценарий включает в себя создание индустриально развитыми государствами современного мира защищенных национальных информационно-коммуникационных сетей. При этом допускается выход информационного контента, не представляющего угрозу национальной безопасности, в глобальную сеть.

«До недавнего времени подобной закрытостью сети отличался только Китай с его знаменитым «великим фаерволом». Но сегодня ряд стран, включая, кстати, и Россию, уже приняли или готовятся принять законы, запрещающие использование иностранных сервисов в ряде случаев. С учетом постоянного роста и усложнения угроз эти стремления будут нарастать, как снежный ком. И законодательное ограничение неизбежно приведет к тем или иным технологическим запретам, прогнозируют многие ведущие эксперты цифровой отрасли»[182].

[182] Там же. С. 9.

При реализации российской политики модернизации системы национальной безопасности Российской Федерации необходимо обратить внимание на следующие моменты.

Во-первых, внутренне информационные магистрали и коммуникационные линии российских органов государственной власти и других государственных учреждений располагаются исключительно в пределах нашей страны, все соответствующие серверы и информационно-коммуникационные узлы находятся также внутри нашей страны, и их информационная безопасность обеспечивается на должном уровне.

Однако, для передачи и накопления информации в российских информационно-коммуникационных сетях используются электронное оборудование иностранного производства. Для обеспечения информационного (цифрового) суверенитета необходимо не только совершенствовать системы защиты магистралей и серверов, использовать отечественное программное обеспечение к ним, но и производить, а также использовать собственное электронное оборудование: компьютеры, телефоны, элементную базу к ним и так далее.[183]

Во-вторых, Российской Федерации, совместно с другими заинтересованными сторонами, необходимо добиваться вывода регулирования Интернета из-под контроля Правительства США. «Как известно, сейчас Еврокомиссия призвала к ограничению влияния Штатов на механику работы Всемирной паутины, и, в частности, на корпорацию «ICANN», которая занимается регулированием доменных имен и адресов в Интернете в глобальном масштабе»[184]. Необходимо активизировать деятельность в этом направлении с привлечением ООН и других заинтересованных международных организаций и государств.

В-третьих, следует не только препятствовать проникновению иностранных государств в российские информационно-коммуникационные сети с целью

[183] Об электронных государственных услугах: Модельный закон МПА СНГ от 7.04.2010 г.
[184] Там же.

шпионажа, но и активно противодействовать информационным диверсиям, Международный опыт показывает, что такая диверсионная деятельность активно ведется американскими спецслужбами против не угодных им правительств и государств. Например, «журналисты агентства «Associated Press» выяснили, что США работали над созданием на Кубе социальной сети, которую можно было бы использовать для подрыва авторитета местных властей. Она стала популярной среди кубинской молодежи. С 2009 года власти США тайно финансировали создание на Кубе местного аналога популярного сервиса микроблогов в Twitter. Ее задачей было ведение антиправительственной пропаганды[185].

В данной связи создание эффективных структур противодействующих диверсиям и психологической агрессии через информационное пространство является одним из важнейших направлений политики модернизации национальной безопасности нашей страны.

2.3. Информационное измерение процесса обеспечения национальной безопасности современной России

Обеспечение национальной безопасности Российской Федерации в условиях современного глобального мира, который несет в себе многочисленные угрозы и вызовы, в том числе направленные и в отношении нашей страны, является сложным и многомерным процессом. В последнее время среди основных измерений данного процесса все в большей мере возрастает значение его информационного измерения.

«Россия стала первым государством, поднявшим на международном уровне (1998) вопрос о появлении принципиально новых – информационных угроз национальной безопасности в XX веке. Очевидно, что происходит трансформация всей военной архитектуры: мы являемся свидетелями «информатизации» вооруженных сил и «интеллектуализации» традиционных вооружений.

[185] США тайно финансировали «кубинский Twitter», чтобы распространять пропаганду // http://russian.rt.com/article/26356 (дата обращения: 15.05.2013)

Информационное оружие становится важным элементом военного потенциала государств. Оно эффективно дополняет традиционные средства ведения вооруженных конфликтов и будет способно, в целом ряде случаев, полностью заменить их»[186].

Таким образом, информационное противоборство в современном мире становится одним из важнейших направлений противодействия сторон друг другу при возникновении международных конфликтов. Методы и средства ведения информационной войны развиваются особенно динамично в наше время. Информационное противоборство происходит в ином пространстве, чем противоборство с применением традиционных видов вооружений.

Это информационное пространство, которое отличает глобальный характер, практическая неистощаемость и быстрая пополняемость информационных ресурсов, возможность их неограниченного копирования и почти мгновенного перемещения на огромные расстояния. Информационные воздействия в определенных случаях трудно идентифицировать и отразить. В связи с указанными выше особыми свойствами информационного пространства в нем применяется и особый вид оружия.

«Информационное оружие – это средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним законных пользователей, дезорганизации работы технических средств, вывода из строя телекоммуникационных сетей, компьютерных систем, всего высокотехнологического обеспечения жизни общества и функционирования государства»[187].

Информационное оружие, в связи с огромными масштабами его применения для боевого воздействия на противника и размером ущерба, который оно может причинить, следует относить к оружию массового поражения. Данное

---

[186] Инновационные направления современных международных отношений / Под ред. А. В. Крутских и А. В. Бирюкова. – М.: Аспект Пресс, 2010. С. 128.

[187] Шеховцев Н. П., Кулешов Ю. П. Информационное оружие: теория и практика применения в информационном противоборстве // Вестник Академии военных наук. 2012. № 1 (38). С. 35.

оружие может применяться в отношении политической и военной элиты противника с целью их дезинформации и введения в заблуждение, для лишения возможности управлять государством, вооруженными силами и другими принципиально важными системами жизнеобеспечения и защиты страны, обеспечения ее национальной безопасности.

«Атакующим информационным оружием сегодня можно назвать:

− компьютерные вирусы, способные размножаться, внедряться в программы, передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и тому подобное;

− логические бомбы – программные закладные устройства, которые заранее внедряют в информационно-управляющие центры военной или гражданской инфраструктуры, чтобы по сигналу или в установленное время привести их в действие;

− средства подавления информационного обмена в телекоммуникационных сетях, фальсификации информации в каналах государственного и военного управления;

− средства нейтрализации тестовых программ;

− различного рода ошибки, сознательно вводимые противником в программное обеспечение объекта»[188].

Прогресс информационно-коммуникационных технологий привел к тому, что из информационного оружия стали выделять новый вид ведения военной борьбы: более узкий, в большей степени связанный с техническими и программными средствами. Данный вид получил название кибероружия.

Это оружие следует отделять от пропагандистских кампаний, психологических операций, политических акций, проводимых через информационное пространство. Применение этого оружия не следует механически связывать с любыми враждебными действиями в Интернете, ориентированными на разрушение информационных систем, имеющих жизненно важное значение.

---

[188] Там же. С. 38.

Не следует также отождествлять кибероружие со всякой дезорганизационной или разрушительной активностью, связанной с информационно-коммуникационной инфраструктурой, в том числе с Интернетом, компьютерами, информационными ресурсамии и магистралями.

В процессе стремительного развития информационно-коммуникационных технологий был создан специальный математический аппарат. Этот аппарат является узкоспециализированным и опирается на теории систем, теории управления, соответствующее математическое обеспечение.

В. В. Каберник следующим образом определяет рассматриваемый вид вооружений: «Под термином «кибероружие» в настоящее время понимают разнообразные технические и программные средства, чаще всего направленные на эксплуатацию уязвимостей в системах передачи и обработки информации или программотехнических системах»[189].

С помощью кибероружия возможно проводить диверсии, в том числе стратегического характера и масштаба. Например, с его помощью можно вызывать программные сбои в компьютерном обеспечении, как военных, так и гражданских систем, имеющих критически важное значение для обеспечения национальной безопасности государства.

Кибероружие – это средство первого удара, имеющее явно выраженный агрессивный, наступательный характер, применяемое в глобальном информационном пространстве и действующее практически мгновенно. В настоящее время не существует систем предупреждения о начале применения такого оружия, что выводит его в разряд наиболее опасных из ныне существующих. В. В. Каберник полагает, что «такие характеристики позволяют приравнять кибероружие к стратегическим наступательным вооружениям. Но разработки и применение кибероружия никак не регламентированы международными соглашениями, что не может не вызывать обоснованных опасений»[190].

---

[189] Каберник В. В. Проблемы классификации кибероружия // Вестник МГИМО-Университета. 2013. № 2. С. 73.
[190] Там же. С. 77.

Кибероружие, исходя из вышеизложенного, можно рассматривать в двух аспектах: в настоящее время, как средство информационного противоборства, и в перспективе, как самостоятельный вид инновационного вооружения.

Таким образом, наличие информационного и кибернетического оружия позволяет рассматривать информационную безопасность не только как важнейший структурный элемент системы национальный безопасности, но и как составляющую часть военной безопасности российского государства.

Одним из первых примеров применения кибероружия стала кибератака иранского ядерного центра, расположенного в городе Натанза (провинция Исфахан, Центральный Иран). В ноябре 2010 года была нарушена работа около тысячи центрифуг для обогащения урановой руды на ядерном заводе в вышеуказанном городе. Эта диверсия была совершена с помощью компьютерной программы Stuxnet.

Данный завод является секретным, однако, в 2007-2008 годах его посещали инспекторы МАГАТЭ. На этом предприятии производились теле- и фотосъемка во время визита туда Президента Ирана Махмуда Ахмадинежада, что позволило организатором кибератаки получить дополнительные сведения о техническом оснащении данного ядерного центра.

Поскольку объект был секретным, то, в целях обеспечения информационной безопасности и кибербезопасности, данный объект не был подсоединен к Интернету. Однако, кибердиверсанты сумели обойти и это препятствие: они использовали для доставки в закрытую секретную сеть внешние носители информации. Для этого хакеры, с помощью электронной почты, внедрили указанную вредоносную программу Stuxnet в компьютеры шести иранских компаний, специализирующихся на разработке программного обеспечения (компьютеры всех этих компаний были подключены к Интернету).

Кибердиверсанты просчитали, что одна или несколько из этих компаний выступают поставщиками программного обеспечения для секретного ядерного завода в Натанзе. Они не ошиблись в своих расчетах. Вредоносная программа в итоге попала в закрытую сеть секретного завода. В результате действия данного

кибероружия управляющие компьютеры на иранском ядерном заводе стали подавать команды, направленные на осуществление действий, которые должны были привести к разрушению технологического оборудования.

Управляющие компьютеры, когда кибердиверсионная программа Stuxnet активизировалась, стали подавать команды сначала на разгон центрифуг для обогащения урана до максимально возможных скоростей вращения, а затем – на их резкое торможение. Пока сотрудники секретного объекта обнаружили, что оборудование ядерного производства работает в аварийном режиме и остановили его, отключив подачу электроэнергии, часть центрифуг оказалась выведенной из строя[191].

Рассмотренный выше пример кибератаки показывает, что при обеспечении информационной безопасности и кибербезопасности большое значение имеет адекватное применение на практике принципа информационной достаточности. Содержание данного принципа раскрывается следующими основными положениями.

Во-первых, недостаток информации может сделать невозможным адекватное и эффективное функционирование системы обеспечения национальной безопасности. Принятие решений и мер по обеспечению безопасности будет либо невозможным, либо недостаточно обоснованным. В то же время, полная информация, ввиду ее огромных объемов и невозможности обработки в приемлемый для принятия решения временной интервал, превращает мероприятия по обеспечению информационной безопасности в лишенные смысла.

Таким образом, существует некоторый критический уровень информационного обеспечения, при достижении которого возможны действия по обеспечению информационной безопасности. Данный уровень обозначается понятием «полнота информации». В данной связи поисковые системы и системы отбора информации и обработки информации, основанные на новейших

[191] Подробнее см.: Степенцев В. Клик победы // Вокруг света. 2013. Июнь. № 6 (2873). С. 36.

компьютерных технологиях, имеют принципиально большое значение для обеспечения рассматриваемого процесса.

Во-вторых, для реализации принципа информационной достаточности необходим целенаправленный и постоянный мониторинг информационных угроз национальной безопасности.

Задачей такого мониторинга, прежде всего, являются обнаружение и прогнозирование возникновения факторов, которые дестабилизируют обстановку в информационном пространстве как на национальном, так и на глобальном уровне. Такие факторы порождают новые угрозы информационного характера для национальной международной безопасности.

В-третьих, среди вышеуказанных факторов особое положение занимают политические. Это связано с тем, что политическая сфера является системообразующим элементом современного общества и государства, а также всей системы международных отношений.

Возникновение информационного общества привело к информатизации политической жизни, к использованию информационно-коммуникационных технологий не только для достижения заданных политических целей и проведения конкретных политических мероприятий, но и, в свою очередь, стало фактором трансформации всей политической жизни обществ развитых государств и мирового сообщества в целом.

Данный процесс набирает силу в наши дни, и появляются все новые его особенности. Так, эксперты отмечают, что в настоящее время явно обозначился процесс формирования «новой информационной элиты», которая с момента своего возникновения активно вмешивается в политическую жизнь общества и стремится потеснить традиционные политические элиты.

Вот, что пишет Д. Л. Сивоволов пишет о формировании новой политической элиты: «Видимая часть айсберга этой проблемы связана со спамерами и хакерами, киберпреступностью. Вполне уместно провести аналогию между американскими бутлегерами, поднявшимися на лифте гигантских противозаконных прибылей в высшую страту американского общества.

Спамеры и хакеры уже вкладывают свои незаконные средства (или не совсем законные в условиях пробелов в информационном праве) в легальные виды бизнеса. Но, кроме них, есть и другие социальные группы, заявившие о своих претензиях на власть. Ассанж и Навальный, как «низвергатели государств», пользуются возможностями современных информационных технологий…

Их много, они пока еще разрознены, но уже имеют огромное технологическое влияние и действуют новыми методами. Для них нет границ, нет законов в традиционном смысле, они действуют очень быстро. Современное государство сегодня может с ними находить общий язык (или бороться в правовом поле), а завтра? Завтра может быть поздно»[192].

Вот почему в современных условиях все большее значение для обеспечения национальной безопасности в информационно аспекте приобретает понятие не просто информационной, а информационно-политической достаточности.

Данный уточненный термин раскрывает роль политического фактора в современных информационных процессах, связанных с обеспечением национальной безопасности при защите от информационных угроз и киберугроз, имеющих политическую природу.

Таким образом, информационное измерение процесса обеспечения национальной безопасности целесообразно рассмотреть сквозь призму системы принципов, имеющих информационно-политический характер. Важное место в этой системе, наряду с принципом информационно-политической достаточности, имеет принцип информационно-политической необходимости.

На принятие своевременных и правильных решений в области обеспечения безопасности как на национальном, так и на глобальном уровнях имеют значение объемы массивов информации, содержащих прогнозы множества вариантов развития событий.

В данной связи Д. И. Полывянный пишет: «Число глобальных форсайтов множится. Сами прогнозы касаются уже не только окружающей среды,

---

[192] Сивоволов Д. Л. Роль российской дипломатии в построении «электронного государства» в Российской Федерации // Вестник МГИМО-Университета. 2013. № 5. С. 56–57.

технологий, экономики и финансов, но и политических, социальных, демографических и иных процессов… Избыток подобного рода материалов, на наш взгляд, иллюстрирует одну характеристику постфактического мира: увеличение объема информации для подготовки и принятия решений в области глобальной безопасности, но дает возможность выбрать ту версию прогноза, которая в наибольшей степени отвечает иным критериям – информационного эффекта, политической целесообразности и пр. Мы получаем возможность того, что нас устраивает, каким бы абсурдным это ни было»[193].

Следовательно, смещение политических процессов в информационное пространство приводит к некоторым очень важным последствиям для обеспечения национальной безопасности. Во-первых, возникает новая квазиреальность, оторванная от реальных политических процессов, но способная взаимодействовать и оказывать влияние на политические процессы в реальном мире и в его традиционном пространстве.

Во-вторых, значительно возрастает роль средств массовой информации, особенно глобальных медийных компаний и интернет-сетей. Они превращаются в новых международных акторов. Они способны оказывать влияние на развитие политических процессов в международном сообществе как на глобальном, так и на региональном уровнях. В связи с этим они реально оказывают воздействие на ситуацию в сфере обеспечения национальной безопасности государств современного мира.

Например, в последнее время обострилась внутриполитическая борьба в Турции, которая в настоящее время переживает непростой переходный период в своем развитии. Особенно обострилось политическое противоборство в этой стране в связи с проведением муниципальных выборов 30 марта 2014 года.

В предвыборной борьбе противники премьер-министра Реджепа Эрдогана и правящей Партии справедливости и развития (ПСР) активно использовали социальные сети для распространения компроматов на Р. Эрдогана и на его

[193] Безопасность на Западе и Востоке и в России: представления, концепции, ситуации: материалы международной научной конференции \ под ред. С. А. Панапина, Д. И. Полывянного. Иваново: Ивановский гос. ун-т. 2013. С. 140–141.

ближайшее окружение. Вследствие этих разоблачений были арестованы сыновья сразу трех министров. В результате трое членов кабмина подали в отставку, еще семерых уволил сам премьер.

Ответом властей стало ужесточение контроля над Интернетом: в стране был заблокирован сначала Twitter, потом –YouTube, силовики получили полномочия закрывать любые сайты без санкции суда. Премьер-министр подал иск в Конституционный суд Турции против ряда социальных сетей. Суть иска – нарушение права Р. Эрдогана и членов его семьи[194].

В-третьих, современные информационно-коммуникационные технологии позволяют множить в виртуальном пространстве гигантские массивы информации, которые затем перетекают в реальное политическое пространство и пространство обеспечения национальной безопасности. В связи с этим возрастает роль процесса отбора информации в области национальной и международной безопасности. Причем такой отбор должен производиться не только по принципу информационной целесообразности, связанной с процессами информационного обеспечения деятельности по обеспечению национальной безопасности. Он должен производиться, исходя из политических и геополитических интересов государства в области национальной безопасности. Таким образом, должен применяться принцип информационно-политической необходимости для поддержания национальной безопасности.

Для характеристики рассмотренного процесса предлагается ввести понятие «информационно-политическая необходимость» необходимое для анализа проблем национальной безопасности.

Понятие информационно-политическая необходимость требует при обеспечении национальной безопасности учета процессов, протекающих в виртуальном пространстве, но оказывающих непосредственное влияние на реальные политические процессы. При этом, в ходе обеспечения национальной безопасности, необходимо принимать во внимание все информационные потоки,

[194] Петров Н. Жизнь после «Твиттера». Почему Эрдоган пока не повторил судьбу Януковича //Русский репортер. 2014. 3–10 апреля. № 13 (341). С. 36–37.

имеющие политическую направленность, и прежде всего – деятельность как традиционных, так и новых медийных сетей глобального и национального масштабов.

Информационно-политическая необходимость тесно связана с понятием информационно-политической достаточности. Необходимость в информационно-политической сфере обеспечивается на определенном уровне, который отвечает сложившимся в каждой конкретной ситуации условиям. Определить этот уровень и параметры информационно-политической достаточности возможно на основе принятия адекватных и эффективных политических решений. При соблюдении этих условий возможно обеспечение информационно-политической устойчивости.

Информационно-политическая устойчивость отражает важные потребности процесса обеспечения национальной безопасности в информационной сфере. В первую очередь это связано с возможностями государства по нейтрализации существующих угроз в информационном пространстве. Решать эту задачу следует на основе эффективной политики путем принятия соответствующих мер в информационно-политической, информационно-технологической и информационно-психологической сферах системы национальной безопасности страны.

Нарушение информационно-политической устойчивости может привести к негативным явлениям и процессам в информационном пространстве, а также в обществе в целом. Данный феномен следует называть информационно-политическим кризисом.

Кризисы в современном обществе многообразны и в состоянии затрагивать все основные области общественного развития. Наиболее часто происходят и достаточно хорошо изучены такие кризисы, как политический и военный, экономический и финансовый, социальный и духовный, экологический и энергетический и другие феномены подобного характера.

Вступление современного общества в информационную фазу развития создало условия для возникновения общественных кризисов, связанных с

информационной сферой жизнедеятельности людей. В настоящее время можно говорить о ярко выраженных проявлениях информационно-политических кризисов как во внутренней жизни отдельных государств (или групп стран), так и на мировой политической арене в целом.

Как было показано ранее, политическая и информационная сферы жизнедеятельности общества и государства оказались тесно взаимосвязаны. Процесс их взаимодействия и сращивания интенсивно продолжается и в наши дни. Это проявляется, прежде всего, во все более масштабном перенесении политических процессов и политической борьбы в информационное пространство.

Одновременно в политических конфликтах все более используются силы и средства информационного противоборства. Вследствие данных процессов возникают кризисы нового формата, которые ранее, до наступления эпохи информационного общества, были просто невозможны. Предлагается обозначить подобного рода явления и процессы понятием «информационно-политический кризис».

В последние годы информационный фактор играет все более возрастающую роль в политических потрясениях и конфликтах, возникающих в разных государствах и регионах современного мира. Первым наиболее ярким проявлением слияния конфронтационных процессов в политической и информационной сферах стали события в Арабском мире в 2011 году и получившие в некоторых средствах массовой информации название «арабская весна».

Ю. В. Косов и С. А. Патаман отмечают: «Спусковым крючком для социальных потрясений в регионе стала «жасминовая революция» в Тунисе. «Аль-Джазира» и социальные сети Интернета широко распространили все перипетии этой революции, вызвав так называемый «эффект домино». Первый раз этот эффект проявился в Египте. По телевидению и online египтяне увидели то, что происходило в Тунисе.

В Египте 30 лет правил Хосни Мубарак. Катарская «Аль-Джазира», ведущая передачи на арабском языке, назвала выборы в этой стране «липой», утверждая, что Мубарак готовит передачу власти своему сыну Гамалю. Тут же египетские власти закрыли популярнейший на Арабском Востоке канал вещания, а 25 января в Каире начались массовые протесты на площади с символичным названием Тахрир, что означает, в переводе с арабского, «Свобода»»[195].

Так называемая «арабская весна» представляет собой первый пример информационно-политического кризиса, который привел к возникновению состояния политического и экономического хаоса в весьма значимом регионе мирового сообщества. Дальше подобные кризисы стали возникать и в других частях мира.

Наиболее опасным для национальной безопасности России стал политический кризис на Украине, составной частью которого следует рассматривать и информационно-политический кризис, связанный с событиями в этом соседнем с нами государстве.

Важной составляющей кризиса на Украине является информационная война, которая развязана захватившей власть в Киеве политической группировкой против своего народа и против Российской Федерации. События на Украине привели и к новому витку охлаждения отношений между нашей страной и Западом.

В данном обострении особо значительную роль играет информационное противоборство. В западных средствах массовой информации введена невиданная цензура на сообщения о политике России в отношении Украины и о событиях внутри самой этой восточноевропейской страны.

Так, пресс-секретарь президента Д. Песков, обсуждая возможность для жителей Европы и Северной Америки узнать правду о позиции России по украинскому кризису, заявил: «Фактически европейские читатели, европейские телезрители сейчас не в состоянии получить всю полноту информации: они

[195] Косов Ю. В, Патаман С. Канал влияния. Почему «Аль-Джазира» побеждает конкурентов в информационной борьбе // Санкт-Петербургские ведомости. 2011. 20 мая. С. 4..

лишены права на свободу выбора информации. Это можно констатировать с большим сожалением, но, тем не менее, это так»[196].

Западная аудитория не может получить правдивую информацию через свои средства массовой информации. Доступ к российским СМИ также практически заблокирован. Дело дошло до чрезвычайной ситуации: высшие лица российского государства пытаются прорвать информационную блокаду, организованную в рамках ведущейся против нашей страны информационной войны. По словам пресс-секретаря, Министр иностранных дел Российской Федерации С. В. Лавров и Президент Российской Федерации В. В. Путин неоднократно пытались донести свою позицию по ситуации в Украине, Однако, в странах Запада делают все, чтобы замолчать российские заявления «Эти объяснения не проходят. Причем не проходят не в силу их несостоятельности – наоборот: позиция очень последовательная и аргументированная. Не проходят потому, что наталкиваются на грубую бетонную стену цензуры», – посетовал Д. С. Песков[197].

Для информационно-политических кризисов характерны следующие наиболее типичные черты:

– такой кризис вызван вынужденными и значительными переменами, которые существенным образом отражаются на функционировании охваченного кризисом объекта;

– информационно-политический кризис является результатом столкновения разно ориентированных политических сил. Причем как минимум одна из таких сил, а, возможно, и все такие силы действуют не только в политической сфере, но и в информационном пространстве. Как правило, преимущество в информационном пространстве приводит к усилению позиций и в политической сфере;

– интернационализация данного кризиса происходит гораздо легче и быстрее, чем традиционных политических кризисов, характерных для исторических периодов, предшествовавших информационной эпохе. Это связано

[196] Песков рассказал о чрезвычайной цензуре в Европе // http://informing.ru/2014/04/16/peskov-rasskazal-o-chrezvychaynoy-cenzure-v-evrope.html (дата обращения: 21.09.2013)
[197] Там же.

с тем, что в отличие от политических пространств, которые ограничены рамками государственных границ, информационное глобальное общество таких границ пока не имеет.

В связи с этим информационное пространство охваченных кризисом стран достаточно доступно для вторжения зарубежных акторов. Только страны, доминирующие в этом пространстве, или государства, способные мобилизовать национальные ресурсы и предпринять экстраординарные меры, способны выстроить информационную защиту своей политической сферы;

− периодичность, конкретные кризисные процессы являются конечными, Однако, выход из кризиса не означает полное устранение этого явления из жизни общества, его повторение уже в новой форме и, как правило, с отличным от предыдущего кризиса содержанием представляется весьма вероятным.

Новый кризис может содержать в себе деструктивные элементы, которые не нашли полного разрешения в ходе предыдущего кризиса и оказались временно ослабленными и приглушенными;

− разрушительность, которая проявляется тем значительнее, чем глубже и острее протекает кризисный процесс, имеющий информационно-политический характер.

Во время серьезных кризисов в результате информационных войн возникает острый недостаток правдивой информации и нехватки сведений о базовых жизнеобеспечивающих ресурсах. Это ведет к деформации и развалу политической системы, социальных институтов и экономики страны.

Особым вниманием со стороны специалистов по разжиганию и конструированию информационно-политических кризисов пользуется постсоветское пространство. Цель таких действий – не допустить развития интеграционных процессов в Евразийском регионе, оттолкнуть от России как можно больше соседних стран и таким образом ослабить позиции нашей страны как мировой державы, полноправного и дееспособного участника глобального политического развития.

Так, Г. Ю. Филимонов по этому поводу пишет: «Особо важное и чувствительное направление работы России, прежде всего на пространстве СНГ, – противодействие активной деятельности США (в их стремлении к реализации проектов на территории государств СНГ в стиле «арабской весны»). Прежде всего это касается многоуровнего блокирования возможности для реализации проектов политтехнологического конструирования враждебных к России режимов по периметру ее границ, организации «бархатных» революций, финансирования антироссийских акций со стороны государств постсоветского пространства и так далее»[198].

Примеров разжигания кризиса на Украине в 2014 году внешними силами, с использованием как прямого вмешательства в дела суверенного государства, так и методов информационной войны, предостаточно. Однако, кризис на Украине имеет и геополитическое глобальное измерение.

Так, в середине апреля 2014 года на сайте НАТО был размещен документ под названием «Обвинение России». Основное содержание этого документа – пропагандистская риторика, выдержанная в духе информационной войны. Интересен он задачами, которые ставятся в заключительной части этого опуса.

В качестве новых стратегических задач альянса теперь называются международная изоляция России, продвижение НАТО на восток, в том числе при размещении системы противоракетной обороны. После этого становится понятным, что грош цена заявлениям Киева о готовности сохранять в дальнейшем внеблоковый статус государства и не размещать на своей территории натовских объектов[199].

Таким образом, следует отметить, что информационно-политический кризис – это общественно-политическое явление, для которого характерны перенос политической борьбы в информационную сферу и использование в политических конфликтах средств информационного противоборства, что

[198] Филимонов Г. Ю. Культурно-информационные механизмы внешней политики США. Истоки и новая реальность. М.: РУДН. 2012. С. 345.
[199] Шестаков Е. Сила есть. Ума бы надо // Российская газета. 2014. 14 апреля. № 84 (6356). С. 7.

порождает возникновение серьезных негативных последствий для национальной безопасности государства.

Противоположностью кризису является устойчивое поступательное развитие государства. В таком состоянии страна способна решать сложные политические и экономические задачи.

В современном информационном обществе важным фактором, обеспечивающим устойчивое развитие, является информационный фактор в его политическом измерении. Ситуация в обществе, когда информационное обеспечение политики, а также политические процессы в информационном пространстве способствуют решению политических проблем и обеспечивают благоприятные условия для развития политической и информационных сфер жизнедеятельности общества, предлагается назвать термином «информационно-политический консенсус».

Такой консенсус означает соглашение значительного большинства членов сообщества относительно наиболее важных принципов организации информационно-политических процессов, а также информационно-политического измерения важнейших процессов и проблем развития государства. При наличии в обществе информационно-политического консенсуса невозможно становится эффективно вести информационную войну, осуществлять информационные диверсии и, в конечном счете, использовать информационное пространство для разрушения политической системы государства.

Показательным примером информационно-политического консенсуса может служить восприятие российским обществом воссоединения Крыма с нашей страной и проблемы защиты соотечественников и русского населения за рубежом, которые могут оказаться в опасности. Так, данные совместного опроса Фонда «Общественное мнение» (ФОМ) и Всероссийского центра изучения общественного мнения (ВЦИОМ) показали, что девять из десяти россиян согласны с тем, что Крым стал частью России.

«Мы видим фантастические цифры. Ни по одному вопросу мы не видели такого единодушия. Это уникально, и это является эмпирическим фактом», –

заявил президент ФОМ А. Ослон. По его словам, 91% респондентов ответили положительно на вопрос: «Согласны ли вы с присоединением Крыма к Российской Федерации в качестве субъекта?» в ходе проведенного опроса с 14 по 16 марта 2014 года во всех регионах России. При этом только 5% от общего количества опрошенных ответили отрицательно, а 4% затруднились с ответом[200].

Информационно-политический консенсус является одним из важных условий – вместе с другими мерами по обеспечению информационной безопасности для осуществления информационно-политического суверенитета государства. Обеспечение в полном объеме национальной безопасности такого государства, как Российская Федерация, а также безопасности российского общества и личной безопасности наших граждан невозможно без осуществления информационного суверенитета нашей страны.

Как известно, суверенитет в наше время – это обязательный атрибут государства. Суверенитет выражается в верховенстве государственной власти по отношению к другим субъектам властных структур внутри государства и независимости на международной арене[201]. Суверенитет распространяется на территорию государства, которая представляет собой ограниченное государственными границами пространство земли и включает сухопутную, морскую, воздушную составляющие, а также недра.

В наше время государственная территория дополняется и виртуальным информационным пространством. Обеспечение безопасности в информационном пространстве должно проходить в правовых рамках без нарушения фундаментального принципа прав человека – свободы доступа к информации. В то же время, государство обязано обеспечивать безопасность общества, государства и личности от угроз исходящих из виртуального пространства. Таким образом, информационный суверенитет превратился в наши дни в важный

---

[200] Худикова Л. Опрос россиян о присоединении Крыма. Цифры – фантастические. / Россия 24. Вести. 2014. 17 марта // http://www.vesti.ru/doc.html?id=1385156 (дата обращения: 26.02.2014)

[201] Политическая наука: Словарь-справочник. сост. проф. Санжаревский И. И. 2010; Политология. Словарь. РГУ. Сост. В. Н. Коновалов. 2010.

компонент государственного суверенитета, и его реализация непосредственно связана с обеспечением национальной безопасности Российской Федерации.

Необходимо отметить, что в современной политической науке не существует четко очерченных понятий «информационный суверенитет», «государственная политика информационного суверенитета». Последние несколько десятилетий выявили различные подходы ряда исследователей, таких как Стариков Н.В.[202], Супрун В.Н.[203], Сергунин А.А.[204], Соловьев Э.Г.[205], Ашманов И.С[206]. и др. к целесообразности введения данных понятий в политико-правовой оборот.

Краеугольным камнем научных споров является вопрос обладает ли «информационный суверенитет» признаками отдельного вида суверенитета или нет.

Понятие «суверенитет» было определено французским мыслителем Жаном Боденом в XIV веке в его труде «Шесть книг о государстве»[207] и характеризовалось как абсолютная и незыблемая власть монарха (суверена) над влиятельными синьорами и парламентами на определенной, четко обозначенной территории. Дальнейшее развитие концепта "суверенитет" относится к периоду XVII-XVIII вв. В трудах философов Томаса Гоббса[208] и Жан Жака Руссо[209] был сделан вывод о том, что суверен может быть не только единоличным, но и коллективным правителем в лице государства. Суверен выступает гарантом прав народа и его верховным судьей. В XIX-XX веках государственный суверенитет определялся как исключительное право на легитимное насилие. Это заключение нашло отражение в трудах немецкого ученого Карла Шмитта «Политическая

---

[202] Стариков Н. В. Дефицит Государственного Суверенитета. http://nstarikov.ru/blog/6047. (дата обращения: 19.05.201)

[203] Супрун В. Н. Теоретико-правовые основы информационного суверенитета. – Дис. на соискание научной степени канд. юрид. наук. – Харьковский национальный университет внутренних дел, Харьков, 2010.

[204] Сергунин А. А. Суверенитет: эволюция концепта. http://www.politex.info/index.phpoption=com_frontpage&Itemid=1. (дата обращения: 10.03.2014)

[205] Материалы международной научно-практической конференции на тему: «Суверенитет государств и концепция «ответственности по защите»: эволюция международной ситуации и интересы России», 30 октября 2013 г. http://www.dipacademy.ru/31.10.13.shtml (дата обращения: 12.11.2013)

[206] Ашманов И. С. Интервью Российской газете: Неделя № 6085 от 23 мая 2013 г.

[207] Боден Ж. Шесть книг о государстве //Антология мировой политической мысли: В 5 т. Т.2. М., 1999. С.689–695.

[208] Гоббс Т. Избранные произведения: в 2 т. М., 1964. Т. 1. 448 с.

[209] Руссо Ж. Ж. Об общественном договоре. Трактаты / Пер. с фр. М.: КАНОН-пресс, Кучково поле, 1998. 416 с.

теология. Четыре главы к учению о суверенитете»[210]. К настоящему времени концепт "суверенитет" прошел долгий путь развития и превратился из узкого понятия абсолютной и незыблемой власти монарха в государстве в основополагающую категорию современных международных отношений.

Суверенитет перестал быть государственно-центричным и наполнился демократическим смыслом:

во внутренней политике – защита прав народа, а не только правителей.

во внешней политике – обеспечение равноправия всех государств в сфере международных отношений.

Попытки представителей ряда политических теорий отрицать ценность концепта «суверенитет» в эпоху глобализации являются несостоятельными и угрожают подорвать сложившиеся к настоящему времени принципы и нормы международного права, которые являются эффективным инструментом обеспечения стабильного развития всего мира.

В конце XX века началось мощное развитие информационно-коммуникационных технологий, резко возрастает роль информационного фактора во всех сферах жизнедеятельности государства, что наполняет понятие «суверенитет» новым содержанием:

во-первых, обеспечение безопасности народов страны, а не только правящей верхушки во внутренней политике;

во-вторых, обеспечение независимой политики всех государств в международном сообществе (во внешней политике).

В ходе проведенного исследования автором проделана работа по систематизации содержания понятия «суверенитет» по его видам: внешний и внутренний и аспектам: государственный, национальный и народный. Раскроем содержание данных понятий.

В целом понятие суверенитет означает – состояние независимости государственной власти от какой-либо иной власти.

---

[210] Шмитт Карл. Политическая теология. М.: Канон-пресс-Ц, 2000. С. 7-98.

Внутренний суверенитет – верховенство и полнота государственной власти по отношению ко всем другим учреждениям в политической системе общества.

Внешний суверенитет – независимость и равноправие государства как субъекта международного права во взаимоотношениях с другими государствами.

Государственный суверенитет – это качественный признак государства, характеризующий его политико-правовую сущность; такое политико-юридическое свойство государственной власти, которое означает ее верховенство и полноту внутри страны, независимость и равноправие во внешнем мире. В свою очередь основными видами государственного суверенитета являются: экономический, идеологический, дипломатический, военный, юридический.

Наряду с государственным суверенитетом используются такие понятия как национальный и народный суверенитет.

Национальный суверенитет – полновластие нации, ее политическая свобода, обладание реальной возможностью определять характер своей национальной жизни.

Народный суверенитет – верховенство народа как источника и носителя власти, его право самому решать свою судьбу.

Охарактеризуем основные элементы, составляющие структуру государственного суверенитета.

Экономический суверенитет – это верховенство государства во внутренних экономических делах и обеспечение экономического равноправия страны среди всех государств мирового сообщества. Если внутри государства не обеспечиваются контрольные функции над своей экономикой, то ее будут контролировать другие зарубежные представители, которые в любой момент смогут обрушить экономику страны или сделать страну сырьевым придатком другого государства или союза государств. В настоящее время развитие подобной ситуации наблюдается на территории Украины.

Идеологический суверенитет определяется наличием своей государственной идеологии, языка и культуры. Если государство не в состоянии иметь собственную идеологию, то обществу такой страны легко можно навязать

любую чуждую культуру, что может привести к потере самого государства. Именно с потерей идеологического суверенитета начался распад такой мощной державы как Союз Советских Социалистических Республик.

Военный суверенитет – безусловное обеспечение безопасности граждан своей страны, общества от внутреннего врага и надежная защита своего государства от внешнего военного нападения. Ослабление военного суверенитета СССР привела к выводу войск из Германии, Польши, Венгрии, краху Организации Варшавского Договора и как следствие, к развалу мощной структуры Вооруженных Сил великой державы.

Дипломатический суверенитет – это возможность государства проводить независимую международную политику. Дипломаты свою деятельность сообразуют всегда с военной мощью государства и развитой экономикой.

Юридический суверенитет – это закрепление статуса суверенного государства в законодательной форме и признание его странами мирового сообщества. Закрепляя законное право на существование государства, он является одним из главных показателей его суверенности.

Следовательно, можно констатировать тот факт, что утрата или ослабление любого из данных основных элементов (группы элементов) государственного суверенитета постепенно приведет к краху государства в целом.

В конце XX начале XXI века значительно усилились процессы глобализации во всех сферах деятельности мирового сообщества, при этом многократно возрос информационный обмен с использованием информационно-коммуникационных технологий как внутри страны, так и за ее пределами. Здесь уместно процитировать слова академика А. И. Берга: «Информация пронизывает все поры жизни и общества»[211]. Таким образом, в эпоху становления и дальнейшего развития информационного общества мы приходим к пониманию необходимости выделения в структуре государственного суверенитета

[211] Кибернетика – неограниченные возможности и возможные ограничения. Современное состояние. – М.: Наука, 1980.– 208 с.

обособленной ее части и определении его понятием как информационный суверенитет.

В современном мире использование новейших информационно-коммуникационных систем в экономике, политике, в военном деле, дипломатии, культуре и других сферах человеческой деятельности приводят все к большей зависимости национальной безопасности страны от обеспечения ее информационной безопасности. Прозрачность государственных границ для информационных потоков в эпоху глобализации и возрастания их объемов ведет к возникновению принципиально новой ситуации, связанной с информационной безопасностью. Создаются предпосылки для возможных нарушений при сборе, накоплении, обработке и распределении информации, что в свою очередь может привести к снижению требуемого уровня информационной безопасности личности, общества и государства.

В «Доктрине информационной безопасности Российской Федерации» сказано: «Интересы государства в информационной сфере заключаются в создании условий для обеспечения суверенитета и территориальной целостности России»[212]. Созданная глобальная информационная сфера привносит в информационный суверенитет и информационную безопасность новые черты: динамизм, быстрый обмен информацией и ее получение в любой точке через сеть «Интернет»; информационная сфера прозрачна, не существует четких границ для потока информации, поэтому в глобальной информационной сфере национальная безопасность и государственный суверенитет требуют принятия дополнительных организационных и технических мер.

При анализе проблемы информационного суверенитета принципиальное значение имеет рассмотрение и изучение проблемы угрозы информационному суверенитету. В общем понимании угроза – это потенциальная возможность нарушения защиты чего-либо или кого-либо. Следствием информационных угроз

[212] Доктрина информационной безопасности Российской Федерации. (Утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895). Гл. 1. Ст. 1 // URL.: http://www.rg.ru/OFICIAL/DOC/MIN_AND_VEDOM/MIM_BEZOP/DOCTR.SHTM. (дата обращения: 27.09.2013)

является ущерб жизненно важным интересам человека, общества и государства в информационной сфере[213].

Основные источники угроз информационному суверенитету следует разделить по источнику их происхождения на две большие группы: внешние и внутренние угрозы.

К внешним угрозам относятся следующие: деятельность политических, экономических, военных, разведывательных и др. структур в информационной сфере, направленных против суверенной власти («холодная информационная война»); доминирование ряда стран в информационном пространстве с целью ущемления национальных интересов России и вытеснения ее с рынка информационно-коммуникационных технологий; деятельность международных террористических организаций; разработка странами Запада, во главе с США, концепций информационного противоборства и др.

К внутренним угрозам относятся следующие: отставание России по уровню и темпам информатизации от ведущих стран Запада и США; недостаточный уровень развития отечественного сектора науки и производства в области информационно- коммуникационных технологий; недостаточная координация со стороны федеральных органов государственной власти процессов информатизации в регионах; несовершенство нормативно-правовой базы и др.

Таким образом, на основании проведенного анализа можно сформулировать понятие информационный суверенитет как верховенство и независимость государственной власти при формировании и реализации информационной политики в национальном сегменте и глобальном информационном пространстве. Принципиальное значение для обеспечения информационного суверенитета имеет государственная информационная политика.

Государственная информационная политика имеет основной целью реализацию национальных интересов государства в области безопасности в информационной сфере.

---

[213] Кучерявый М. М., Вус М. А., Шакин Д. Н., Юсупов Р. М. Эскиз системного подхода к формированию понятийного аппарата информационной безопасности // Информатизация и связь. 2012. № 9. С. 22–24.

В свою очередь под информационной сферой понимается «совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений»[214].

Данная политика реализуется в информационно-технологической, информационно-психологической и информационно-политической сферах.

Информационный суверенитет предполагает наличие:

– в информационно-технологической сфере («цифровой» суверенитет) – собственного технологического цикла, программно-аппаратной платформы, поисковой и навигационной систем, сетевого оборудования и средств защиты информации отечественного производства, национального сегмента сети "Интернет" и социальных сетей, национальной платежной системы и др.;

– в информационно-психологической сфере («ментальный» суверенитет) – национальной идеи, высокого уровня информационной культуры и образованности общества;

– в информационно-политической сфере («властный» суверенитет) – внятной информационной политики, правительства народного доверия, патриотически-настроенной элиты, средств массовой информации, ориентированных на защиту национальных интересов, устойчивой национальной валюты и др.

Составной частью и принципиально важным базовым элементом информационной политики является государственная политика информационного суверенитета.

Государственная политика информационного суверенитета представляет собой деятельность государства по осуществлению самостоятельной информационной политики на основе существующих законов страны и норм международного права в информационной сфере с целью обеспечения

[214] Доктрина информационной безопасности Российской Федерации. (Утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895) // URL.: http://www.rg.ru/OFICIAL/DOC/MIN_AND_VEDOM/MIM_BEZOP/DOCTR.SHTM (дата обращения: 27.09.2013)

верховенства информационной безопасности личности, общества и государства внутри страны и ее независимости в глобальном информационном пространстве.

Государственная политика информационного суверенитета достигается деятельностью государства по следующим направлениям:

1) Определением геополитических информационных интересов страны в условиях глобализации всех сфер деятельности человечества (экономика, политика, идеология, дипломатия, вооруженные силы, культура и образование).

2) Создание нормативно-правовой базы, гарантирующей информационный суверенитет личности и общества, а на международной арене – участие в создании и развитии норм международного права в обеспечение информационного суверенитета государства.

3) Образование национальных (государственных и социальных) защищенных информационных сетей и систем, способных безопасно взаимодействовать с глобальным информационным пространством.

4) Создание собственных сил и средств в области информационно-коммуникационных технологий.

5) Образование информационных войск, оснащенных современными средствами информационно-коммуникационных технологий для достижения целей и решения задач информационного противоборства.

6) Проведение широкой международной дипломатической деятельности по обеспечению информационного суверенитета страны на международной арене.

7) Контроль информационных потоков, как внутри страны, так и поступающих извне с целью ограничения информации, пропагандирующей чуждые ценности (Рисунок 5).

Рисунок 5 – Информационный суверенитет. Политика информационного суверенитета

* * *

В завершении данного раздела диссертации считаем целесообразным сделать следующие выводы.

Во-первых, под влиянием факторов глобального развития, а также причин научно-технологического характера произошло преображение процессов обеспечения национальной безопасности. Они приобрели инновационный, комплексный и динамичный характеры. В данных условиях потребовалась качественно новая форма координации сил и средств, обеспечивающих безопасность на всех уровнях.

Роль такого координатора была возложена на советы безопасности как на важнейшие государственные органы, действующие на национальных уровнях. Таким образом, произошли существенные системные изменения в обеспечении национальной безопасности, имеющие институционально-политическое измерение.

Во-вторых, в наши дни произошла информатизация всей системы национальной безопасности. Одновременно человечество в наше время столкнулось с созданием, в дополнение к реальному миру, существующему испокон веков в физическом пространстве, мира, который возник и развивается в виртуальном информационном пространстве.

Такие изменения привели к тому, что информационная безопасность стала выступать в качестве одного из ведущих факторов системных изменений в структуре и содержании национальной безопасности в целом. На международном уровне процессы обеспечения информационной безопасности в мировом сообществе заняли центральное место в усилиях человеческого сообщества по поддержанию международной безопасности.

В-третьих, в условиях современной России, перешедшей на информационную стадию развития, обеспечение информационной безопасности имеет принципиальное значение для успешного функционирования всей системы национальной безопасности. Для этого требуется реализация последовательной политики модернизации системы национальной безопасности нашей страны.

Одной из основ этой политики должен быть принцип информационной достаточности. Применение данного принципа означает превращение информационной безопасности в системообразующий элемент национальной безопасности России; обеспечение современными инновационными информационно-коммуникационными технологиями всех важнейших институтов и систем российского общества; достижение эффективной защищенности всех информационных ресурсов и коммуникаций, используемых в нашей стране.

В-четвертых, предлагается ввести понятие «информационно-политическая безопасность». Это связано с интеграцией политической и информационной сфер общественной жизни: постоянное возрастание роли информационного фактора в политике, усиление воздействия Интернета на политическое развитие общества, доминирование США в глобальном информационном обществе ведет к утрате сбалансированности и устойчивости развития информационного общества, а также и мировых политических процессов.

В-пятых, политику модернизации системы национальной безопасности России в информационном измерении следует осуществлять по трем основным направлениям: информационно-технологическому, информационно-психологическому и информационно-политическому.

При проведении данной модернизации необходимо принимать во внимание три возможных сценария развития Интернета в среднесрочной перспективе: первый – сохранение статус-кво в этой глобальной системе; второй – распад глобальной сети Интернет на региональные и национальные системы, гораздо меньших масштабов и обособленные друг от друга различными защитными и контрольными структурами; третий – создание индустриально развитыми государствами современного мира защищенных национальных информационно-коммуникационных сетей, которые допускают выход информационного контента, не представляющего угрозу национальной безопасности, в Глобальную сеть.

В-шестых, в системе обеспечения информационной безопасности особое место занимают политические факторы. Это связано с тем, что политическая сфера является системообразующим элементом современного общества и государства, а также всей системы международных отношений.

Возникновение информационного общества привело к информатизации политической жизни, к использованию информационно-коммуникационных технологий не только для достижения заданных политических целей и проведения конкретных политических мероприятий, но и, в свою очередь, стало фактором трансформации всей политической жизни обществ развитых государств и мирового сообщества в целом.

В-седьмых, для теоретического анализа и разработки практических рекомендаций по обеспечению национальной безопасности в информационно-политическом измерении предложено ввести в политическую науку новые понятия:

– «информационно-политическая необходимость», согласно которой, при обеспечении национальной безопасности необходимо учитывать процессы,

протекающие в виртуальном пространстве, но оказывающие непосредственное влияние на реальные политические процессы.

− «информационно-политическая устойчивость» – это способность государства осуществлять политику нейтрализации существующих угроз в информационном пространстве с целью обеспечения безопасности в информационно-политической, информационно-технологической и информационно-психологической сферах системы национальной безопасности страны.

− «информационно-политический кризис», связанный с переносом политической борьбы в информационное пространство и с использованием в политических конфликтах сил и средств информационного противоборства, что ведет к возникновению кризисов нового формата, которые ранее, до наступления эпохи информационного общества, были просто невозможны.

− «информационно-политический консенсус», означающий соглашение значительного большинства членов сообщества относительно наиболее важных принципов организации информационно-политических процессов, а также информационно политического измерения важнейших проблем развития государства.

В-восьмых, на основе комплексного политологического анализа политических процессов в современном глобальном мире, оказывающих непосредственное влияние на национальную безопасность Российской Федерации предложено дальнейшее развитие концепта «государственный суверенитет», с введением в его содержание новых категорий политической науки: "информационный суверенитет" и "государственная политика информационного суверенитета".

Впервые раскрыто содержание категории «информационный суверенитет». В отличие от ряда исследователей автор диссертации включил в его содержание кроме известного информационно-технологического («цифрового») суверенитета два новых элемента: информационно-психологический («ментальный») и информационно-политический («властный») суверенитеты. В диссертационной

работе предложен механизм практической реализации «информационного суверенитета» в виде «государственной политики информационного суверенитета» и сформулированы ее основные направления.

3. ВЛИЯНИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

Обеспечение безопасности нашей страны от угроз, направленных против ее национальной безопасности, представляет собой важную задачу как в практическом, так и в теоретическом аспектах. Актуальность и сложность этой задачи возрастает при рассмотрении ее применительно к информационному пространству в новых геополитических условиях второго десятилетия XXI века.

Во-первых, информационное пространство становится все в большей степени связанным с мировыми геополитическими процессами. Вопросы формирования и развития глобального информационного общества находятся в фокусе мировой политики.

Во-вторых, прогресс в развитии информационно-коммуникационных технологий открывает принципиально новые возможности как для устойчивого роста экономики, так и для укрепления обороноспособности современных наиболее развитых государств. Таким образом, развитие информационной сферы представляет собой важное направление политики модернизации российского государства.

В то же время постоянное расширение возможностей информационно-коммуникационных технологий, все большая зависимость от их успешного применения всех основных сфер общественной жизни постоянно повышают уязвимость современного высокоразвитого государства к угрозам его национальной безопасности, которые возникают в глобальном информационном пространстве.

В современных условиях информационная безопасность рассматривается как важная составляющая системы обеспечения национальной безопасности личности, общества и государства. Сформированы теоретические основы данного вопроса. Однако, роль и место информационной безопасности в системе обеспечения национальной безопасности Российской Федерации, в политической жизни нашего

общества и политическом курсе государства, направленном на защиту наших национальных интересов, требуют дальнейшего осмысления.

Политика информационной безопасности Российской Федерации не может рассматриваться изолированно от долгосрочной стратегии развития информационного общества в Российской Федерации. Вопросы политики информационной безопасности регулярно обсуждаются на заседаниях Совета Безопасности Российской Федерации. При этом авторитетном органе государственного управления Указом Президента Российской Федерации от 6 мая 2010 года № 590 создана Межведомственная комиссия по информационной безопасности[215].

Таким образом, политика информационной безопасности, являясь важной составной частью политики национальной безопасности нашей страны, имеет комплексный характер, связана с основными сферами жизнедеятельности российского общества и геополитическими процессами в современном мире. Данная политика требует изучения как с теоретической, так и с практической точек зрения. В центре такой политики находится процесс обеспечения безопасности нашей страны в глобальном информационном пространстве

3.1. Анализ концептуальных основ политики национальной безопасности

Национальная безопасность Российской Федерации обеспечивается в результате целенаправленной деятельности государственных и общественных институтов, а также граждан по выявлению, предупреждению угроз безопасности личности, общества и государства и противодействию им в качестве обязательного и непременного условия защиты национальных интересов России.

Эта деятельность определяется политикой национальной безопасности Российской Федерации. Процесс обеспечения национальной безопасности нашей

[215] См.: Положение о межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности // Конституционно-правовой статус Совета Безопасности Российской Федерации / Под общ. ред. Н. П. Патрушева. – 2-е изд., испр. и доп. М.: Издательство «Известия». 2013. С. 263–266.

страны включает в себя как деятельность российского государства, так и всего общества и каждого гражданина России в отдельности.

Она направлена на защиту национальных интересов нашей страны, а также на практическую реализацию данных интересов. «Национальные интересы Российской Федерации» – совокупность внутренних и внешних потребностей государства в обеспечении защищенности и устойчивого развития личности, общества и государства»[216].

Политическое руководство Российской Федерации ставит цели и формулирует задачи по защите и разработке форм, методов и принципов достижения вышеуказанных целей, исходя из учета национальных интересов нашей страны на мировой арене. Политика национальной безопасности осуществляется на основе следующих принципов:

- соблюдения строгой законности;
- обеспечения баланса интересов личности, общества и государства;
- соблюдения взаимной ответственности личности, общества и государства за национальную безопасность;
- интеграции с международными системами коллективной безопасности как в глобальном, так и региональном измерениях.

Основные направления политики национальной безопасности Российской Федерации определяются национальными интересами нашей страны. При определении данных направлений учитываются также потребности разработки и использования эффективных средств противодействия внешним и внутренним угрозам национальным интересам.

Достижение главных целей политики национальной безопасности обеспечивается на основе выполнения комплекса соответствующих взаимосвязанных задач во всех основных сферах жизнедеятельности российского общества. Эти задачи ставятся и решаются в рамках соответствующих документов стратегического планирования.

---

[216] Стратегия национальной безопасности Российской Федерации до 2020 г. Утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537 // Российская газета.. 2009. 19 мая. Гл. 1. Ст. 6.

К таким документам относятся концепции долгосрочного развития (например, «Концепция долгосрочного социально-экономического развития Российской Федерации»). В систему документов стратегического планирования в нашей стране также входят:

- программы развития отдельных секторов национальной экономики;
- концепции развития федеральных округов;
- комплексные программы социально-экономического развития субъектов Российской Федерации;
- межгосударственные программы, в выполнении которых принимает участие Россия;
- федеральные и ведомственные целевые программы;
- государственный оборонный заказ и некоторые другие концепции и доктрины, имеющие стратегический характер для обеспечения национальной безопасности.

В «Стратегии национальной безопасности Российской Федерации до 2020 года» отмечено: «Система документов стратегического планирования… концепции, доктрины и основы (основные направления) государственной политики в сферах обеспечения национальной безопасности и по отдельным направлениям внутренней и внешней политики государства формируется Правительством Российской Федерации и заинтересованными федеральными органами исполнительной власти с участием органов государственной власти субъектов Российской Федерации на основании Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации»[217].

Таким образом, для того чтобы эффективно проводить политику национальной безопасности, государством формируется система документов стратегического планирования и главные направления деятельности в указанной сфере, на основе которых определяются и реализуются первоочередные задачи данной политики.

---

[217] Там же. Гл. V. Ст. 101.

С позиций сегодняшнего дня и перспектив процесса обеспечения национальной безопасности Российской Федерации одной из важнейших практических задач в данной сфере, непосредственно связанной с повышением эффективности политики национальной безопасности, представляется становление системы ее критериев, показателей и оценок.

«В области обеспечения национальной безопасности, – по мнению экспертов Совета Безопасности Российской Федерации, – в отечественной теории и практике единый подход к методологии оценки ее состояния только формируется. Это обусловлено тем, что национальная безопасность, структурированная по стратегическим национальным приоритетам и входящим в них различным сферам национальной безопасности, является комплексной и одновременно достаточно многофакторной категорией. В свою очередь, установление взаимовлияния стратегических национальных приоритетов, содержащих сферы национальной безопасности, в динамике их взаимосвязанного развития, само по себе представляет достаточно сложную научно-практическую проблему» [218].

Для оценки состояния национальной безопасности прежде всего важен процесс мониторинга этого феномена. Под таким мониторингом понимают систему наблюдения и анализа определяющих изменений в сфере национальной безопасности в результате воздействия внешних и внутренних факторов.

В процесс мониторинга производятся сбор, регистрация и исследование информации о поведении ключевых параметров изучаемого объекта с целью получения выводов о его поведении и состоянии. Для получения данных выводов в случае национальной безопасности необходимо, чтобы количество характеризующих этот феномен признаков было небольшим: по возможности, предельно компактным.

[218] Конституционно-правовой статус Совета Безопасности Российской Федерации / Под общ. ред. Н. П. Патрушева. – 2-е изд., испр. и доп. М.: Издательство «Известия», 2013. С. 24–25.

В качестве основных признаков и параметров при рассматриваемом мониторинге используют критерии и показатели оценки состояния национальной безопасности.

«Критерии оценки состояния национальной безопасности – совокупность признаков, которыми характеризуется такое общественно-политическое и социально-экономическое явление, как национальная безопасность, и которые выступают в качестве правила (средства для суждения, мерила) на основании которого выносится суждение или производится оценка этого явления»[219].

Таким образом, рассматриваемые критерии представляют собой признаки, на основании которых производится оценка, определение и классификация явлений и процессов в сфере национальной безопасности и оценка состояния всей этой сферы в целом. Критерии также выступают мерилом такой оценки.

Автором разработаны и предложены методики квалиметрических оценок в политических науках:

- методика регрессивного анализа ущерба;
- методика нахождения квалиметрических показателей на основе линейных сверток для комплексных количественных оценок в политических науках;
- методика оценки возможного ущерба государству из вероятностной модели событий[220].

Обсуждаемые критерии должны обеспечивать качественную оценку состояния национальной безопасности и процесса ее обеспечения. Такая оценка опирается на определенные показатели, которые имеют как количественный, так и качественный характеры.

В пространство национальной безопасности входят все основные сферы общественной жизнедеятельности. К ним относится политическая, экономическая, социальная, международная, духовная, военная, экологическая, научно-образовательная, информационная и некоторые другие сферы

[219] Там же. С. 27.
[220] См. Приложение А.

общественного развития. Роль информационной сферы в процессе обеспечения национальной безопасности в последние годы постоянно возрастает.

Эта сфера достаточно легко поддается формализации и измерению с помощью количественных показателей, Однако, некоторые сферы общественной жизнедеятельности – такие, как политическая, духовная и международная, – достаточно трудно поддаются формализации, и использование количественных показателей может быть в данном случае ограничено.

Критерии оценки состояния национальной безопасности должны соответствовать условиям осуществления эффективного мониторинга в данной сфере и быть сопоставимы с другими системами мониторинга, включающими как оценки уровня развития Российской Федерации в целом, так и с учетом индикаторов продуктивности и оперативности ведомственной деятельности.

Обсуждаемые критерии должны иметь интегративный характер, иметь обобщающее и комплексное содержание. Данные критерии должны создавать условия для объективности выводов оценок и рекомендаций по всем вопросам состояния и обеспечения национальной безопасности Российской Федерации.

В свою очередь, критерии раскрываются и выражаются в наиболее полном виде, адекватном отражаемому процессу с помощью показателей. «Показатели оценки состояния национальной безопасности (показатели национальной безопасности, основные характеристик состояния национальной безопасности) – обобщенные количественные или качественные характеристики, с помощью которых можно оценить состояние национальной безопасности, используя их предельные (критические, пороговые) значения»[221]. В связи с этим следует подчеркнуть, что сущность национальной безопасности раскрывается в системе, состоящей из ее критериев и показателей.

Количественные показатели могут служить в качестве индикаторов определенных процессов в сфере безопасности. Под индикаторами обычно понимают доступную для наблюдения и измерения характеристику какого-либо явления или процесса в сфере национальной безопасности, позволяющих судить о

[221] Там же С. 27–28 .

других характеристиках этих явлений или процессов, не доступных непосредственному исследованию.

Наименьшая возможная величина индикатора, за которой наступает граница проявления какого-либо негативного процесса (или явления), называется порогом (или пороговым значением) показателя. Для мониторинга национальной безопасности особенно важны пороговые значения индикаторов.

Так, Л. П. Гончаренко и Е. С. Куценко, применительно к экономической безопасности, подчеркивают: «Для экономической безопасности важное значение имеют не сами показатели, а их пороговые значения: то есть предельные величины, несоблюдение значений которых препятствует нормальному ходу развития различных элементов воспроизводства, приводит к формированию негативных, разрушительных тенденций в экономической безопасности»[222].

На основе показателей, по которым можно определить пороговые значения, формируется система индикаторов экономической безопасности. Особенно важна эта система для осуществления мониторинга рассматриваемого феномена. Самый высокий уровень обеспечения безопасности возможно достигнуть и поддерживать в условиях, когда значения всех соответствующих индикаторов не выходят за допустимые границы их пороговых величин.

Данные показатели образуют индикационную систему, отражающую характеристики процессов и явлений в сфере безопасности. Эти процессы и явления взаимосвязаны и взаимозависимы, что отражается и в соотношении их характеристик. Важно отметить, исходя из этого обстоятельства, что пороговые величины определенного индикатора, отражающего одну соответствующую характеристику, не могут достигаться путем оказания негативного влияния на другие индикаторы, а значит, – и на отражаемые ими характеристики процессов и явлений в сфере безопасности.

[222] Гончаренко Л. П., Куценко Е. С. Управление безопасностью. М.: Изд-во «Кронус». 2010. С. 40–41.

В отечественных исследованиях по экономической безопасности к настоящему времени выполнены достаточно интересные разработки показателей, в том числе и индикаторов экономической безопасности[223].

Данный опыт может быть распространен и на ряд других составляющих национальной безопасности с учетом их специфики реализации на практике и особенностей их научно-теоретического изучения и оперативного анализа.

Наряду с разработками в рамках теории экономической безопасности, для формирования теоретико-методологических подходов к созданию аналитического инструментария для оценки состояния сферы национальной безопасности существенное значение имеют исследования, связанные с развитием теории управления стратегическими рисками[224].

Для мониторинга всей сферы национальной безопасности в указанных исследованиях используют категории «критерии безопасности» и «показатели безопасности», для которых также определяют пороговые величины.

Группой экспертов Совета Безопасности Российской Федерации под руководством Н. П. Патрушева «сформирован Перечень критериев и показателей национальной безопасности Российской Федерации, который нацелен на измерение эффективности достижения конкретного результата по каждому стратегическому национальному приоритету применительно к различным сферам национальной безопасности (внутриполитическая, экономическая, социальная, науки и образования, международная, духовная, и информационная, военная и

---

[223] См.: Глазьев С. Ю. Основа обеспечения экономической безопасности страны: альтернативный реформационный курс // Российский экономический журнал. 1997. № 1. С. 8–9; Денежкина И. Е., Суздалева Д. А. Система показателей для мониторинга экономической безопасности региона // Эффективное антикризисное управление. 2011. № 3 (66). С. 142–148; Прокопов Б. И. Сущность и содержание экономической безопасности // Проблемы современной экономики. 2008. № 4 (28); Богомолов В. А. Экономическая безопасность. М.: ЮНИТИ, 2010; Положение о межведомственной комиссии Совета Безопасности Российской Федерации по безопасности в экономической и социальной сфере. // Собрание законодательства Российской Федерации. 2011. № 19. Ст. 2721 и так далее.

[224] См.: Стратегические риски России: оценка и прогноз / под общ. ред. Ю. Л. Воробьева. М.: Деловой экспресс, 2005. 392 с.; Осипов В. И. Опасные природные процессы – стратегические риски России. М.: РБОФ «Знание» им. С.И. Вавилова, 2009. 40 с.; Вишняков Я. Д., Радаев Н. Н. Общая теория рисков. 2-е изд., испр. М.: Издательский центр «Академия», 2008. 368 с.; Кривошапка И. Без страха перед рисками // Эффективное антикризисное управление. 2012. № 4 (73). С. 5–10; Глущенко Ю. Н. Стратегические риски России в условиях продолжающегося мирового экономического кризиса: нефтегазовый фактор //Военно-политическая ситуация в мире и вопросы обеспечения национальной безопасности России / под ред. Г. Г. Тищенко и Е. С. Хотьковой. М.: РИСИ, 2011. С. 49–57 и так далее.

оборонно-промышленная, экологическая, общественной безопасности) с помощью 17 критериев, объединяющих 83 показателя»[225].

Для данных показателей определены пороговые значения. Они понимаются как предельно допустимые значения данных индикаторов, выход за пределы которых порождает серьезные угрозы и открывает возможности для их практического осуществления, а также приводит к возникновению негативных тенденций в развитии страны (или отдельных областей жизнедеятельности общества и социальных институтов).

Для конкретных сфер национальной безопасности пороговые значения соответствующих показателей имеют свои конкретную методику определения и специфику проявления. Однако, важно, чтобы эти индикаторы могли коррелировать друг с другом в рамках комплекса показателей национальной безопасности России.

Таким образом, система критериев и показателей национальной безопасности Российской Федерации непосредственно направлена на обеспечение мониторинга реальных и потенциальных угроз стабильному и устойчивому развитию нашей страны. В данной связи при анализе концептуальных основ политики национальной безопасности следует отметить, что одной из центральных категорией выступает понятие «угроза национальной безопасности.

В «Стратегии национальной безопасности Российской Федерации до 2020 года» этому понятию дано следующие определение: «Угроза национальной безопасности» – прямая или косвенная возможность нанесения ущерба конституционным правам, свободам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию Российской Федерации, обороне и безопасности государства»[226].

Таким образом, угрозы национальной безопасности могут проявляться в каждой основной сфере жизнедеятельности российского общества. Они способны

---

[225] Конституционно-правовой статус Совета Безопасности Российской Федерации / под общ. ред. Н.П. Патрушева. 2-е изд., испр. и доп. М.: Издательство «Известия», 2013. С. 27.

[226] Стратегия национальной безопасности Российской Федерации до 2020 г. Утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537 // Российская газета.. 2009. 19 мая. Гл. 1. Ст. 6.

нести потенциальную и реальную опасность для базовых устоев государства, социума, конкретных социальных групп и каждого отдельного гражданина Российской Федерации.

Данные угрозы могут иметь как природное происхождение, так и могут быть порождены деятельностью человека и цивилизацией, созданной его гением. В зависимости от характера опасности и источника причинения ущерба, выделяют три основные группы угроз национальной безопасности: естественно-природные, техносферные и антропогенные.

1) Естественно-природные угрозы имеют происхождение, связанное с совокупностью естественных условий на Земле или в каком-либо регионе нашей планеты. Эти условия включают геологические процессы, климат, рельеф, растительный и животный мир и так далее.

В последнее время эксперты стали обращать особое внимание на потенциальные угрозы жизни на нашей планете, которые зарождаются в недрах космического пространства. На протяжении всей истории в мире дикой природы возникали угрозы, вызванные силами природной стихии и реализация которых вызывала серьезные катастрофы. В наше время стихийные бедствия продолжают наносить серьезный ущерб всем странам и народам.

Однако, в прошлом столетии значительно возросло негативное воздействие человека на окружающее среду, что вызвало экологический кризис в отношениях общества и природы. Эту ситуацию достаточно точно характеризовал Ж.-И. Кусто, когда написал: «Прежде природа угрожала человеку, а сейчас человек угрожает природе». Подобное нерациональное воздействие на природную среду служит источником возникновения новых угроз национальной безопасности.

2) Угрозы, имеющие техногенный характер, возникают в искусственной среде, созданной человеком в процессе развития цивилизации. Существует целый ряд отраслей народного хозяйства, которые имеют особо опасный характер. К ним относят:

– транспорт, включая, в первую очередь, суда с ядерными движительными установками, супертанкеры, перевозящие колоссальные объемы углеводородных

энергоносителей и других опасных веществ, пассажирские перевозки и тому подобное;

− энергетика, особенно атомные электростанции, линии передач электричества, гидроэлектростанции и другие потенциально опасные энергетические объекты;

− космическая отрасль, использующая ракетоносители и космические аппараты, в которых в значительных количествах применяются вредные для здоровья людей и природы вещества.

Указанные выше и некоторые другие объекты и процессы техносферы относятся к источникам повышенной опасности: то есть они, из-за особых технико-функциональных характеристик, при наступлении непредвиденных и непреодолимых чрезвычайных обстоятельств могут выходить из-под контроля и причинять серьезный ущерб.

3) Антропогенные угрозы связаны с агрессивной деятельностью зарубежных государств и их институтов, включая силовые структуры и спецслужбы, а также с враждебными действиями отельных индивидов, групп лиц или организаций, которые могут быть как внутренними, так и иностранными, в том числе международными.

Враждебные воздействия со стороны указанных субъектов могут происходить в различных сферах общественной жизнедеятельности, в каждой из которых они имеют свои особенности. По этой причине антропогенные угрозы принято разделять на определенные группы в зависимости от области их проявления. Наиболее значимыми и опасными являются следующие из них: военные, политические, экономические, информационные, духовные, социальные и некоторые другие.

Угрозы национальной безопасности достаточно часто проистекают из нескольких источников, и при их реализации наносится ущерб, имеющий сложный, комплексный характер. Например, катастрофа в марте 2011 года на японской атомной электростанции «Фукусима 1», которая входила в число 25 крупнейших АЭС в мире, была вызвана необычайно редким сочетанием последовательной

реализации в кратчайший срок угроз естественно-природного и техногенного характера. Возникла ситуация, которую не смогли предусмотреть проектировщики.

Террористическая деятельность может наносить ущерб, имеющий политический, экономический, социальный, международный и иной характеры. Следует признать справедливым вывод, который сделал А. А. Борщ: «Для эффективной деятельности системы национальной безопасности государства необходима правильная оценка угроз национальной безопасности в современных условиях»[227].

Для объективной оценки рассматриваемых угроз требуются соответствующая их диагностика и анализ. В данной ситуации проведение эффективной политики национальной безопасности невозможно без ранней диагностики и предварительного анализа факторов стратегических рисков, приводящих к возникновению угроз стабильному и устойчивому развитию Российской Федерации и имеющих разную природу возникновения и характер проявления.

Эти факторы можно объединить в несколько групп разного уровня. При такой систематизации факторы, входящие в группу каждого верхнего уровня, обуславливают генерирование факторов, находящихся на последующих ступенях при рассмотрении схемы развития данного процесса сверху вниз.

В качестве факторов, обуславливающих состояние сферы национальной безопасности, выделяются следующие: противоположность и столкновение национальных интересов, возможности нанесения ущерба, угрозы и вызовы, стратегически приоритеты, точки и зоны уязвимости, стратегические риски, парирование угроз и ущерб или последствия.

Рассмотрим эти факторы более подробно. Важную роль в контексте национальной безопасности играют национальные интересы, которые, как известно, выражают внутренние и внешние потребности государства в обеспечении защищенности и устойчивого развития. Состояние защищенности и устойчивости распространяется, в первую очередь, на личность, общество и само

[227] Борщ А. А. Национальная безопасность и власть. М.; РАНХиГС при Президенте Российской Федерации, 2012. С. 56.

государство. При реализации национальных интересов возникают определенные противоречия, которые, с одной стороны, носят объективный характер, так как вызваны противоречиями общественного развития, отражающих способность нашего государства к изменениям и модернизации. С другой стороны, данные противоречия порождаются субъективными причинами. Они отражают противоборство между основными акторами международных отношений за более выгодные позиции в глобальном развитии и более высокий статус в мировой политике и экономике.

Таким образом, противоречия во внешней и внутренней сферах, обусловленные комплексом причин объективного и субъективного характера, порождают противоположность интересов различных политических сил, участвующих в общественных процессах, как на международном, так и внутригосударственном уровнях.

Данные противоречия могут оказывать позитивное влияние на развитие нашего государства, когда их разрешение способствует реализации инновационных подходов к достижению новых качественных уровней в основных сферах общественной жизнедеятельности. В то же время, некоторые из подобных противоречий могут негативно воздействовать на функционирование российского общества.

При анализе национальной безопасности России в соответствии с темой исследования, внимание преимущественно будет обращено на противоречия негативного характера и именно в этом смысле будет использоваться указанный термин.

При рассмотрении данной проблемы следует обратить внимание на то, что обсуждаемые противоречия ведут к возникновению противоположных национальных интересов у России и некоторых других субъектов международных отношений, находящихся в конкурентных отношениях с нашей страной (или вследствие других причин, имеющих, например, геополитическую, историческую или противоправную природу).

В данной связи в «Стратегии национальной безопасности Российской Федерации до 2020 г.» дан следующий прогноз: «На обеспечение национальных интересов Российской Федерации негативное влияние будут оказывать вероятные рецидивы односторонних силовых подходов в международных отношениях, противоречия между основными участниками мировой политики, угроза распространения оружия массового уничтожения и его попадания в руки террористов, а также совершенствование форм противоправной деятельности в кибернетической и биологической областях, в сфере высоких технологий»[228].

При реализации оппонентами России в мировых политических процессах подходов, подобных тем, на которые указывается в приведенном выше документе, может возникать столкновение интересов. При этом на практике выявить негативные противоречия, полностью раскрыть их природу, определить основные источники этих противоречий и их носителей в современных мировых и региональных политических процессах оказывается достаточно затруднительно. Эти процессы являются сложными и взаимосвязанными, имеют многофакторный и многомерный характер.

Группа российских экспертов из Института проблем управления РАН, изучая аналогичные вопросы на примере Арктической зоны России, пришла к следующему выводу: «Внешние противоречия определяются, прежде всего, различием в целевых установках и национальных интересах различных государств и отчетливо проявляются в экономической и политической сферах, в области международных отношений, а также в информационной сфере и так далее. Следует отметить, что в большинстве практических случаев достаточно трудно идентифицировать противоречия и их носители (субъекты), что неизбежно влечет принятие неэффективных решений, усугубляющих эти противоречия, либо порождающих новые с соответствующими негативными последствиями»[229].

---

[228] Стратегия национальной безопасности Российской Федерации до 2020 г. Утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537 // Российская газета. 2009. 19 мая. Гл. 1. Ст. 10.

[229] Шульц В. В., Кульба В. В., Шелков А. Б., Чернов И. В. Диагностика и сценарный анализ угроз социально-экономическому развитию Арктической зоны Российской Федерации. М.: Институт проблем управления РАН, 2012. С. 13–14.

Столкновение интересов на международной арене при определенных обстоятельствах ведет к возникновению прямых (или косвенных) возможностей для нанесения ущерба участникам такой коллизии. Ущерб может быть материальным и нематериальным.

Под материальным ущербом понимают урон государственному имуществу и собственности физических лиц и негосударственных организаций, убытки, непредвиденные расходы и иные финансовые и вещественные потери. Нематериальный ущерб проявляется в нанесении ущерба национальным интересам субъекта международных отношений, которые не имеют обычного вещественно-стоимостного выражения.

Эти интересы могут иметь политический (или даже геополитический) характер, иметь дипломатическую, духовную или моральную природу. В результате подрывается международный авторитет пострадавшего субъекта, его геополитические позиции в мире в целом или в конкретном международном регионе, создаются проблемы для его эффективной внешней политики и устойчивого внутреннего развития.

Ущерб бывает прямой: когда неблагоприятные последствия наступают непосредственно для национальной безопасности государства, подвергнувшегося политическому (или иному) давлению. Подобные последствия могут быть вызваны косвенным порядком: путем отрицательного влияния через третью сторону или проведения недружественных акций в скрытой форме, истинные организаторы которых действуют через подставных лиц. В конечном счете, негативное воздействие таким образом может оказываться и на стабильность всего мирового порядка.

Итак, следует отметить, что анализ ситуаций, при которых возникают прямые или косвенные возможности для нанесения ущерба национальным интересам Российской Федерации, играет важную роль при проведении диагностики угроз безопасности нашей страны. Большое значение имеют угрозы геополитического характера.

В начале текущего столетия к границам нашей страны с Запада приблизились мощные военно-политическая (НАТО) и экономическая (ЕС) группировки, некоторые члены которых имеют исторические конфликты с Россией или еще недавно предъявляли к ней территориальные претензии. Отношения нашей страны с НАТО и ЕС складываются достаточно сложно. Периоды определенного сближения и поиска баланса интересов сменяются фазами нарастания противоречий, а в случае с Северо-Атлантическим альянсом – и обострения отношений.

На востоке продолжает претендовать на часть российских земель одно из наиболее развитых в экономическом отношении государств мира – Япония. Несколько лет назад территориальные претензии правящих кругов нашего восточного соседа вспыхнули с новой силой. После смены правительства в Стране восходящего солнца ситуация в российско-японских отношениях стабилизировалась, Однако, от рецидивов новых столкновений интересов по поводу так называемых «северных территорий» никто не застрахован.

Вдоль значительной части государственной границы Российской Федерации сохраняется внешний пояс продолжающихся (или обостряющихся) региональных и локальных конфликтов. Данные геополитические реалии таят в себе огромные потенциальные угрозы национальной безопасности России.

В «Концепции внешней политики Российской Федерации (редакция 2013 г.)» проанализированы основные вызовы и угрозы национальной безопасности Российской Федерации, среди которых, в плане нашего исследования, существенное значение имеют следующие выводы: «Опасность для международного мира и стабильности представляют попытки регулировать кризисы путем применения вне рамок Совета Безопасности ООН одностороннего санкционного давления и иных мер силового воздействия, включая вооруженную агрессию…

На первый план в современной международной политике выходят имеющие трансграничную природу новые вызовы и угрозы, стремительно возрастают их уровни, диверсифицируются их характер и география.

Прежде всего, это опасность распространения оружия массового уничтожения и средств его доставки, международный терроризм, неконтролируемый трафик оружия и боевиков, радикализация общественных настроений, провоцирующая религиозный экстремизм и этноконфессиональные антагонизмы, нелегальная миграция, морское пиратство, незаконный оборот наркотиков, коррупция, региональные и внутренние конфликты, дефицит жизненно важных ресурсов, демографические проблемы, глобальная бедность, экологические и санитарно-эпидемиологические вызовы, изменение климата, угрозы информационной и продовольственной безопасности»[230].

Таким образом, даже краткий анализ основных вызовов и угроз безопасности Российской Федерации показывает, что существенную роль в их природе и содержании играет военная составляющая. Прогнозы развития военно-политической обстановки в мире на среднесрочный период, предпринятые российскими исследователями, показывают, что вблизи границ России активизируется противоборство за доступ к природным, энергетическим, научно-техническим, людским и другим ресурсам на постсоветском пространстве, а также за расширение возможностей, в том числе легальных, по их использованию.

Во всемирном масштабе будет нарастать глобальная нестабильность, порождаемая, с одной стороны, стремлением Соединенных Штатов сохранить чрезвычайно выгодную для них модель мирового устройства, сложившуюся в 1990-е гг., а, с другой, усилиями держав – региональных лидеров увеличить свое влияние на мировые процессы и способствовать, таким образом, продвижению многополярной системы устройства международного сообщества.

В данном контексте серьезную озабоченность вызывают и российско-американские отношения. Например, эксперт Института проблем международной безопасности А. Фененко считает, что «российско-американские отношения находятся в состоянии вялотекущей конфронтации. Во-первых, между сторонами нет содержательного диалога по вопросам ПРО/СНВ. Во-вторых, между лидерами

[230] Концепция внешней политики Российской Федерации. Утверждена Президентом Российской Федерации В.В. Путиным 12 февраля 2013 г. Гл 2. Ст. 15–16. URL: http://www.ln.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255. (дата обращения: 14.09.2013)

России и США полтора года не было полноценной рабочей встречи. В-третьих, «Закон Магницкого» доказал, что Соединенные Штаты начинают отрицать легитимность определенного сегмента российской элиты. Москва, судя по ее действиям, намерена реагировать адекватно»[231].

Оценка угроз национальной безопасности должна производиться в соотношении со стратегическими национальными приоритетами, с учетом имеющихся точек и зон уязвимости. Под стратегическим национальными приоритетами понимаются важнейшие направления обеспечения национальной безопасности Российской Федерации. Эти направления определяются в рамках принципиальных крупномасштабных и ориентированных на долговременную перспективу решений, касающихся развития нашей страны.

Данное развитие должно носить устойчивый характер, обеспечивать стратегическую стабильность России и ее союзников. Согласно мнению экспертов Совета Федерации ФС РФ В. Ю. Кравченко и В. В. Щипалова, «на формирование стратегических приоритетов оказывают влияние следующие факторы:

− стратегическое видение, стратегическая миссия и стратегические цели экономического, политического и социального развития государства;

− экономические, политико-дипломатические, социальные и военные стратегические программы и национальные проекты по обеспечению реализации жизненно важных национальных интересов государства;

− стратегические риски деятельности (или бездеятельности) по реализации национальных интересов»[232].

Итак, важным фактором формирования стратегических национальных приоритетов являются стратегические риски. Они означают вероятность возникновения неблагоприятного развития ситуации. Такой подход отражает,

---

[231] Фененко А. «Белый дом подчеркнул свое нежелание вести диалог с администрацией Владимира Путина». 12 августа 2013 г. // http://russiancouncil.ru/blogs/debate/?id_4=614 (дата обращения: 12.03.2014)

[232] Кравченко В. Ю. Щипалов В. В. Стратегические приоритеты в сфере национальной безопасности // Аналитический вестник Совета Федерации ФС РФ. 2010. № 17 (403). С. 29.

прежде всего, наличие потенциальной угрозы, которая означает вероятность наступления негативных последствий.

Стратегические риски связаны с определением перспектив крупномасштабных процессов, имеющих принципиальное значение для развития государства. Кроме масштабов проявления, стратегические риски могут иметь как допустимый по тяжести последствий, так и критический уровни.

Критический уровень может быть обусловлен кризисными ситуациями, например, в развитии мирового сообщества. Критический риск, если содержащаяся в этом феномене угроза реализуется, может привести к очень серьезным (и даже катастрофическим!) последствиям.

Вот почему при оценке потребностей обеспечения национальной безопасности необходимо наиболее адекватными способами оценивать потенциальные угрозы, содержащиеся в стратегических рисках, а также использовать наиболее эффективные методы парирования таких угроз и объективно прогнозировать возможные последствия развития ситуации в сложившихся критических условиях.

3.2. Роль и место информационной составляющей в системе политики обеспечения национальной безопасности Российской Федерации

Политика национальной безопасности Российской Федерации в научно-теоретическом аспекте базируется на соответствующих концептуальных основах, а в практическом измерении реализуется с помощью системы обеспечения национальной безопасности. Данная система охватывает политическую и экономическую, духовную и информационную, социальную и экологическую и некоторые другие стороны жизни общества.

В систему обеспечения национальной безопасности входят соответствующие силы и средства. К силам обеспечения национальной безопасности в нашей стране в современных условиях относят:

− Вооруженные Силы Российской Федерации, другие войска, воинские формирования и органы, в которых федеральным законодательством предусмотрена военная и (или) правоохранительная служба;

− федеральные органы государственной власти, принимающие участие в обеспечении национальной безопасности государства на основании законодательства Российской Федерации.

Силы обеспечения национальной безопасности проводят конкретную практическую работу по применению комплекса надлежащих мер для обеспечения национальной безопасности Российской Федерации. В настоящее время особое внимание уделяется как традиционным сферам – военной, оборонно-промышленной, экономической безопасности, так и инновационному направлению: информационной безопасности.

Силы, о которых идет речь, также принимают участие в оптимизации нормативно-правовой базы и модернизации институциональной структуры национальной безопасности. Действия органов и учреждений, входящих в силы обеспечения национальной безопасности, направлены также на повышение статуса нашей страны в международном сообществе, улучшение ее имиджа в окружающем мире, а также на усиление влияния и значения нашей страны в процессе решения проблем глобального развития.

В состав средств обеспечения национальной безопасности, являющих другим важным компонентом рассматриваемой системы обеспечения безопасности, входят:

− технологии, основанные на передовых достижения научно-технического прогресса и имеющие как узкоспециализированное назначение для сферы безопасности, так и двойное назначение: то есть средства, которые могут применяться и в других областях общественной жизнедеятельности;

− технические, программные, лингвистические, правовые, организационные средства;

− телекоммуникационные каналы, используемые в системе обеспечения национальной безопасности для сбора, формирования, обработки, передачи или

приема информации о состоянии национальной безопасности и мерах по ее укреплению.

Стремительное и широкое распространение современных информационных технологий происходит не только в сфере национальной безопасности, но в смежных с ней областях, которые имеют принципиальное значение для обеспечения безопасности современного государства.

«В данной связи нельзя не отметить стремительное распространение информационных технологий в производственных системах, – пишет Л. В. Панкова, – которое привело к кардинальной модификации материально-технической базы по созданию оборонной продукции серьезным организационно-управленческим преобразованиям»[233].

Таким образом, роль информационной составляющей в системе национальной безопасности в начале XXI века значительно возросла, и этот процесс продолжается и в настоящее время. Особое значение имеет информационная компонента средств обеспечения национальной безопасности. Очевидно, что ее удельный вес в этом процессе будет возрастать и далее – по крайней мере, в обозримом будущем.

Значительная часть сил обеспечения национальной безопасности также ориентирована на решение стратегических задач непосредственно (или косвенным образом) связанных с решением задач по обеспечению информационной безопасности. Для управления и координации действий указанных сил и использования названных средств в информационной области в нашей стране проводится соответствующая политика.

«Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной

[233] Панкова Л. В. Военно-экономическое обеспечение безопасности: инновационное измерение // Вестник Московского университета. Серия 25. Международные отношения и мировая политика. 2012. № 2. С. 23.

сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере»[234].

В структуре политики информационной безопасности целесообразно выделить два основных направления: государственно-правовое и технологическое.

Государственно-правовое направление связано с функционированием государственных органов власти и состоянием законодательной и нормативно-правовой баз, с качеством человеческого фактора и потенциала, с развитием общественных отношений.

В «Доктрине информационной безопасности Российской Федерации» сформулированы основные принципы, направления и задачи государственной политики обеспечения информационной безопасности Российской Федерации. Они поставлены перед федеральными органами государственной власти, органами государственной власти субъектов федерации, общественными объединениями. В указанном документе значительное внимание уделяется гуманитарному направлению политики обеспечения национальной безопасности, реализации роли человеческого фактора в этом процессе.

В частности, в Доктрине подчеркивается: «Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности Российской Федерации…

Правовое обеспечение информационной безопасности Российской Федерации должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере»[235].

Федеральные органы государственной власти и органы государственной власти субъектов Российской Федерации при решении возникающих в

---

[234] Доктрина информационной безопасности Российской Федерации. Гл. III. Ст. 8 // http://www.rg.ru/OFICIAL/DOC/MIN_AND_VEDOM/MIM_BEZOP/DOCTR.SHTM. (дата обращения: 27.09.2013)

[235] Там же.

информационной сфере конфликтов должны неукоснительно руководствоваться указанными принципами, а также иными законодательными нормативными и правовыми актами, регулирующими отношения в сфере информационной безопасности.

Важнейшей задачей государства в области информационной безопасности является обеспечение гарантий конституционных прав и свобод человека и гражданина на доступ к информации и обеспечение полноценных возможностей для деятельности в информационной сфере.

Аналогичная правовая практика существует и во многих зарубежных странах. В законодательных и нормативных документах ведущих государств современного мира информационная безопасность определяется в качестве реальной возможности информационной системы проявлять, в должной степени, устойчивость к аварийным ситуациям и противозаконным враждебным действиям, которые в состоянии ограничить или закрыть доступ к хранимой или транслируемой информации, а также нарушить ее сохранность и конфиденциальность.

Как показывает анализ зарубежного опыта правового обеспечения информационной безопасности, около 100 государств приняли законы о праве на информацию. Устойчивая тенденция на принятие национальных законов, гарантирующих доступ к информации о деятельности органов власти, отмечается с начала 60-х годов ушедшего столетия.

В последние 20 лет такие законы были приняты во Франции, Греции, Дании, Голландии, Бельгии, Португалии, Испании, Финляндии и в Италии. Законы о доступе граждан к правительственной информации приняты в США, Канаде, Австралии и Новой Зеландии.

В ряде стран Европы – таких, как Нидерланды, Испания, Португалия, Австрия, Венгрия, Эстония, Бельгия и Румыния, – право граждан на доступ к официальной информации закреплено конституционно. Во Франции, Греции и в Италии эти права закреплены в законах.

Совершенствование законодательства в данной сфере продолжается в Великобритании, Германии, Эстонии, Молдове, Польше и ряде других государств. Законодательное ограничение прав на доступ к правительственной информации установлено, например, в Швеции и Финляндии [236].

Интересен для нашей страны опыт Европейского Союза по созданию системы правового регулирования телекоммуникации и защиты информации. В рамках этой системы принят комплекс соответствующих правовых актов, направленных на обеспечение информационной безопасности. В частности, было введено понятие «сетевая и информационная безопасность» (СИБ) и сформулированы концептуальные основы европейской политики по ее обеспечению, приняты директивы Европейской комиссии о частной жизни и электронных коммуникациях.

В ЕС, наряду с принятием нормативно-правовых актов, проводится работа по институционализации сферы информационной безопасности. Так, учрежден институциональный контрольный механизм за соблюдением прав граждан на частную жизнь при обработке персональных данных институтами и органами Евросоюза в составе Европейского контролера по защите данных и инспекторов по защите данных. В контексте системы мер по борьбе с угрозами СИБ организовано Европейское агентство сетевой и информационной безопасности.

Приняты ЕС и документы принципиального стратегического характера: в частности, Стратегия безопасности информационного общества «Диалог, партнерство и расширение возможностей». Данная Стратегия содержит обзор современного состояния угроз безопасности информационного общества и определяет дополнительные меры по обеспечению СИБ.

К документам подобного рода следует отнести также акт «Защита Европы от крупномасштабных кибератак и сбоев: повышение готовности, безопасности и устойчивости», который содержит инициативу по защите важнейшей

[236] См.: Асланов Р. М. Зарубежный опыт правового регулирования обеспечения информационной безопасности // Политика и общество. 2012. № 2 (86). С. 46.

информационной инфраструктуры. В последнее время в ЕС запущены несколько важных инновационных проектов в сфере противодействия киберпреступности[237].

Однако, в условиях развития информационного общества в нашей стране и достижением процесса информатизации глобальных масштабов становится все более очевидным, что обеспечить информационную безопасность путем деятельности органов государственной власти, правоохранительных структур и развития законодательной и нормативно-правовой базы достаточно затруднительно. Полностью не решает эту проблему даже применение инновационных технических средств.

В современном информационном обществе имеет место обусловленность всех основных видов индивидуальной и общественной деятельности от информационно-коммуникационных технологий. От этих технологий зависит информационное обеспечение государственной деятельности, деловой активности, сфер образования, культуры и так далее. Таким образом, информационный контент превратился в важный и ценный компонент функционирования всех основных субъектов общества: личности, социальных и экономических институтов, государства.

Когда имеющую большое значение информацию не удается должным образом защитить от несанкционированного доступа, возникают проблемы с обеспечением безопасности на личном, общественном или государственном уровне.

В связи с рассмотренной выше проблемой специалисты обращают внимание на необходимость формирования соответствующей современным реалиям информационного общества культуры информационной безопасности.

Например, А. А. Малюк по данному поводу пишет: «Государственные органы, предприятия, организации, индивидуальные владельцы и пользователи IT-индустрии должны знать о факторах, угрожающих информационной безопасности, и возможных превентивных действиях, должны осознавать свою

[237] Подробнее см.: Смирнов А. А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского союза. М.: ЮНИТИ. ДАНА: Закон и право. 2012. С. 77–110.

ответственность и принимать меры для повышения безопасности информационных технологий. С этой целью должна быть сформирована культура информационной безопасности, которая является составной частью культуры общества»[238].

В современном мире прилагаются значительные усилия для формирования глобальной культуры кибербезопасности. Это свидетельствует о том, что обеспечение информационной безопасности превратилось в актуальную глобальную проблему наших дней. Данный процесс следует рассматривать в одном ряду с проблемами сохранения и развития культуры и предотвращения войн и вооруженных конфликтов, обеспечения экономической и экологической, демографической и продовольственной, энергетической и сырьевой безопасности в планетарном масштабе (Рисунок 6).

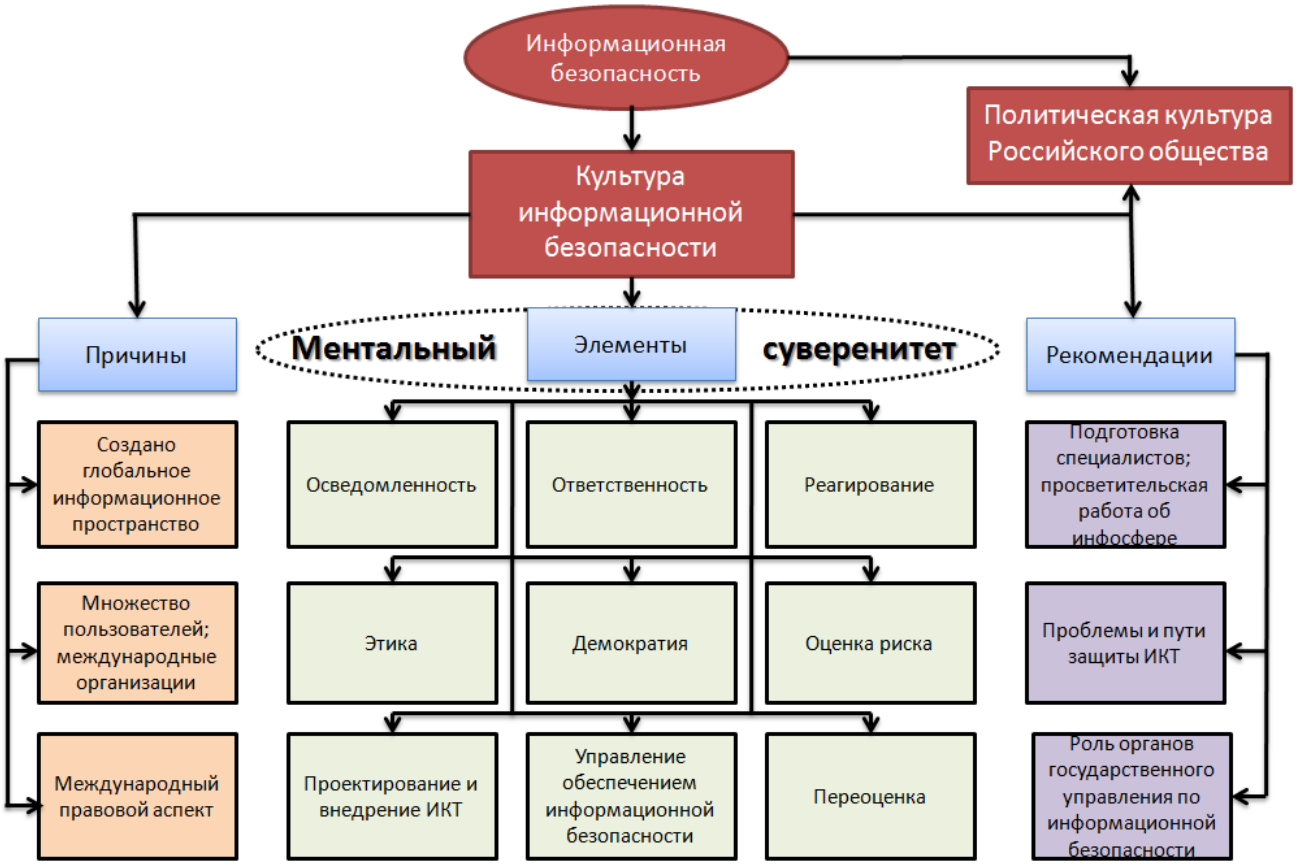


Рисунок 6 – Политические аспекты культуры информационной безопасности

[238] Малюк А. А. Формирование культуры информационной безопасности общества // Педагогика. 2009. № 3. Март 2009. С. 33.

Основным дипломатическим полем для разработки подходов к формированию глобальной культуры кибербезопасности стали ведущие международные организации. Такая ситуация объясняется следующими причинами.

Во-первых, это связано с тем, что в современном глобальном информационном обществе все больше становится трансграничных соединений, связывающих пользователей в разных странах, порой находящихся на разных континентах и расположенных на расстояниях в тысячи и тысячи километров друг от друга.

Во-вторых, поиски решения проблемы глобальной культуры информационной безопасности требуют переговоров с большим числом участников – субъектов международных отношений и международного права. Подобного рода форумы многосторонней дипломатии наиболее оптимально, как показывает опыт, проводить в рамках международных организаций.

В-третьих, на повестке дня, как мы можем предположить, – создание нового института международного публичного права: права информационной безопасности. Как известно, международное право формируется в наше время, прежде всего, ООН и некоторыми другим авторитетными международными организациями.

Организация Объединенных Наций одной из первых проявила большой интерес к рассматриваемой проблеме. С одной стороны, культура глобальной безопасности имеет большое значение для обеспечения безопасности всего международного сообщества. С другой стороны, ООН всегда проявляла пристальное внимание к вопросам развития информационного обмена и информационных технологий.

Например, еще в 1971 году Генеральная Ассамблея Объединенных Наций приняла резолюцию «Свобода информации; права человека и научно-технический прогресс». Дважды (в 2000 и 2001 гг.) этот авторитетный форум рассматривал вопросы и принимал резолюции на тему «Борьба с преступным использованием информационных технологий».

В плане исследования особый интерес вызывают резолюции Генеральной Ассамблеи ООН по проблемам формирования культуры информационной безопасности. Первая из них, под названием «Создание глобальной культуры кибербезопасности», была принята 20 декабря 2002 года.

Эксперты и дипломаты Организации Объединенных Наций констатировали: «Стремительное развитие информационных технологий изменило то, как государственные органы, предприятия, другие организации и индивидуальные пользователи, которые разрабатывают эти информационные системы и сети, … должны подходить к кибербезопасности»[239].

В Приложении к этому документу сформулированы «Элементы для создания глобальной культуры кибербезопасности». По мнению авторов данного документа, глобальная культура кибербезопасности будет требовать от всех участников учета следующих взаимодополняющих элементов:

– осведомленность. Участники должны быть осведомлены о необходимости безопасности информационных систем и сетей, а также о том, что они могут сделать для повышения безопасности;

– ответственность. Участники отвечают за безопасность информационных систем и сетей сообразно с ролью каждого из них. Участники должны подвергать свои политику, практику, меры и процедуры регулярному обзору и оценивать, соответствуют ли они среде их применения;

– реагирование. Участники должны принимать своевременные и совместные меры по предупреждению инцидентов, затрагивающих безопасность, их обнаружению и реагированию на них. Они должны обмениваться в надлежащих случаях информацией об угрозах и факторах уязвимости и вводить процедуры, предусматривающие оперативное и эффективное сотрудничество в деле предупреждения таких инцидентов, их обнаружения и реагирования на них.

---

[239] Резолюция, принятая Генеральной Ассамблеей. № 57/239. Создание глобальной культуры кибербезопасности. 20 декабря 2002 г. // http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N03/ 06/54/PDF/N0350654.pdf?OpenElement. (дата обращения: 13.02.2014)

Это может предполагать трансграничный информационный обмен и сотрудничество;

− этика. Поскольку информационные системы и сети проникли во все уголки современного общества, участникам необходимо учитывать законные интересы других и признавать, что их действия (или бездействие) могут повредить другим;

− демократия. Безопасность должна обеспечиваться так, чтобы это соответствовало ценностям, которые признаются демократическим обществом, включая свободу обмена мыслями и идеями, свободный поток информации, конфиденциальность информации и коммуникации, надлежащую защиту информации личного характера, открытость и гласность;

− оценка риска. Все участники должны выполнять периодическую оценку риска, которая: позволяет выявлять угрозы и факторы уязвимости; имеет достаточно широкую базу, чтобы охватить такие ключевые внутренние и внешние факторы, как технология, физические и человеческие факторы, применяемая методика и услуги третьих лиц, сказывающиеся на безопасности; дает возможность определить допустимую степень риска; помогает выбрать надлежащие инструменты контроля, позволяющие регулировать риск потенциального ущерба информационным системам и сетям с учетом характера и значимости защищаемой информации;

− проектирование и внедрение средств обеспечения безопасности. Участники должны рассматривать соображения безопасности в качестве важнейшего элемента планирования и проектирования, эксплуатации и использования информационных систем и сетей;

− управление обеспечением безопасности. Участники должны принять комплексный подход к управлению обеспечением безопасности, опираясь на динамичную оценку риска, охватывающую все уровни деятельности участников и все аспекты их операций;

− переоценка. Участники должны подвергать вопросы безопасности информационных систем и сетей обзору и повторной оценке и вносить

надлежащие изменения в политику, практику, меры и процедуры обеспечения безопасности, учитывая при этом появление новых и изменение прежних угроз и факторов уязвимости[240].

Итак, анализ основных элементов, необходимых для формирования культуры информационной безопасности, показывает, что в них достаточно ярко выражен политический аспект. Прежде всего, речь идет о политических ценностях демократического общества, а также о характеристиках политического управления: таких, как политика обеспечения безопасности, ответственность и оценка рисков.

В данной связи можно утверждать, во-первых, что культура информационной безопасности тесно соприкасается с политической культурой российского общества и в перспективе будет оказывать определенное влияние на развитие последней. Во-вторых, необходимо, чтобы процесс формирования культуры кибербезопасности занял должное место в информационной составляющей политики национальной безопасности Российской Федерации.

Почти через 10 лет Генеральная Ассамблея ООН вновь вернулась к обсуждаемой проблеме и приняла новую резолюцию, в которой, в частности, дано описание «Инструмента добровольной самооценки национальных усилий по защите важнейших информационных инфраструктур».

В рекомендациях, содержащихся в документе, акцент сделан на защиту, в первую очередь, систем государственного управления, а также на просветительскую работу по распространению знаний об информационной сфере и подготовке специалистов-профессионалов для этой сферы.

Так, одна из рекомендаций, изложенная в вышеуказанном «Инструменте добровольной самооценки», ориентирует государства – члены Организации Объединенных Наций на подготовку и реализацию «плана кибербезопасности».

Этот план предназначен «для систем, управление которыми осуществляет правительство, национальных программ повышения уровня осведомленности и распространения знаний среди, в частности, детей и индивидуальных

[240] Там же.

пользователей, а также о потребностях в профессиональной подготовке в области национальной кибербезопасности и защиты важнейших информационных инфраструктур»[241].

Международный союз электросвязи (МСЭ), который является специализированным учреждением ООН в области электросвязи и информационно-коммуникационных технологий, также активно подключился к работе по формированию культуры информационной безопасности.

Как уже отмечалось ранее, Генеральная Ассамблея ООН делает акцент на международном сотрудничестве по рассматриваемой проблеме. В то же время, в докладе МСЭ «Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности» обращается внимание на решение вопроса о формировании данной культуры на национальном уровне[242].

Для достижения этой цели предлагается выработать соответствующие национальные подходы. Они должны быть достаточно гибкими, поскольку существующие национальные возможности обеспечения кибербезопасности постоянно меняются, а угрозы информационной сфере непрерывно совершенствуются.

Эксперты МСЭ констатируют: «С учетом того что персональные компьютеры становятся все более мощными, что происходит конвергенция технологий, что все шире распространяется применение ИКТ и что растет число соединений через государственные границы, все, кто разрабатывает, владеет, управляет, обслуживает и использует информационные сети, должны осознавать проблемы кибербезопасности и принимать соответствующие их функциям меры для защиты сетей. Органы государственного управления должны играть ведущую

---

[241] Резолюция, принятая Генеральной Ассамблеей. № 64/211. Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур. 21 декабря 2009 года // http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/474/51/PDF/N0947451.pdf?OpenElement. (дата обращения: 18.10.2013)

[242] Следует отметить, что Международным союзом электросвязи подготовлена «Глобальная программа кибербезопасности (ГПК) МСЭ. Основа для международного сотрудничества в области кибербезопасности». Женева: МСЭ, 2008 // http://www.ifap.ru/pr/2008/080908aa.pdf. (дата обращения: 07.02.2014)

роль в создании культуры кибербезопасности и в поддержке мер, принимаемых другими участниками»[243].

Соединенные Штаты являются государством, которое во второй половине прошлого века создали наиболее благоприятные условия для развития у себя информационно-коммуникационных технологий и стали одной из первых стран, где эти технологии широко используются во всех сферах общественной жизни.

США уделяют большое внимание политике информационной безопасности, активно развивая как государственно-правовое, так и технологическое направления указанной сферы. В плане настоящего исследования представляет интерес значительный разрыв между этими направлениями, возникший на определенном этапе развития глобального информационного общества.

Эксперты отмечают, что огромный прогресс в развитии информационно-коммуникационных технологий привел к тому, что их прогресс стал опережать формирование соответствующей нормативно-правовой базы. Значительные усилия государственная власть США прилагает к преодолению этого разрыва.

Данный опыт развития политики информационной безопасности в заокеанской державе, вероятно, может быть учтен при формировании политики информационной безопасности и в нашей стране. Российские исследователи уделяют достаточно большое внимание анализу американского опыта реализации политики обеспечения информационной безопасности[244].

Однако, в последнее время политика информационной безопасности США оказалась серьезно скомпрометирована разоблачениями со стороны некоторых сотрудников американских спецслужб, и прежде всего – Э. Сноуденом. Достоянием всеобщей гласности стали обстоятельства и факты, которые неопровержимо свидетельствовали о том, что американские правящие круги при

---

[243] Доклад Международного союза электросвязи «Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности». Женева: МСЭ, 2010 // http://www.itu.int/dms_pub/itu-d/opb/stg/D-STG-SG01.22-2010-PDF-R.pdf. (дата обращения: 19.02.2014)

[244] См., например: Шариков П. А. Эволюция государственной стратегии в сфере информационной безопасности // США – Канада. Экономика, политика, культура. 2009. 3 12. С. 95–108; его же, Подходы демократов и республиканцев к информационной безопасности // Россия и Америка в XXI в.: электронный научный журнал. 2012. № 1 // http://www.rusus.ru/?act=read&id=312. (дата обращения: 11.11.2013)

проведении политики информационной безопасности полностью пренебрегали стратегическими интересами в сфере кибербезопасности других государств.

«Сноуден предал гласности информацию о секретной программе электронной слежки под кодовым названием «PRISM». И надо подчеркнуть, что речь идет, в том числе, о слежке за европейскими пользователями интернет-компаний и социальных сетей. АНБ является главным оператором программы, распределяя полученную информацию (по сферам интересов) между ЦРУ, ФБР, Управлением по борьбе с наркотиками и другими спецслужбами.

Сноуден раскрыл далеко не все секреты, которыми владеет, но и то, что прозвучало, в Латинской Америке, например, было воспринято с крайней тревогой. Если Империя позволяет себе нагло шпионить даже за своими союзниками по НАТО, то на какие действия она способна в странах к югу от Рио-Гранде (город в штате Техас, США), которые считает своим «задним двором»?»[245].

В начале данного параграфа мы, наряду с государственно-правовым направлением, выделили и вторую линию информационной политики российского государства, которую обозначили как технологическую. Данные разоблачения показали тесную взаимосвязь между двумя этими направлениями политики информационной безопасности.

Если ведущая иностранная держава пренебрегает государственными интересами других стран и нормами внутреннего и международного права, то неадекватная технологическая политика в сфере информационной безопасности и недостаточная материально-техническая кибербаза могут поставить под угрозу национальную безопасность государства.

В сложившихся условиях в глобальном информационном пространстве, когда, в силу политики США, возникли серьезные проблемы с обеспечением кибербезопасности у многих других стран, Российская Федерация должна найти

[245] Тарасов Е. Информационная безопасность США в опасности. 04.07.2013 // http://newsland.com/news/detail/id/1207288. (дата обращения: 18.01.2014)

адекватный ответ на эти глобальные вызовы. Российская Федерация должна реализовать долгосрочную технологическую политику в информационной сфере.

Целью такой политики должно стать создание информационно-коммуникационной инфраструктуры, в которую входили бы собственные информационные магистрали. Эти магистрали должны включать систему серверов, созданных и расположенных на территории России и управляемых российскими компаниями. Российским должны быть все компоненты указанной инфраструктуры, начиная от процессоров и операционных систем и заканчивая конкретными программными продуктами.

В «Государственной программе Российской Федерации «Информационное общество (2011–2020 гг.)» обращается внимание на то, что в современном глобальном информационном обществе отставание в развитии информационно–коммуникационных технологий и киберпространства представляет угрозу не только обеспечению информационной безопасности, но и всей системе поддержания национальной безопасности.

Это означает, что недостаточно эффективная политика информационной безопасности становится слабым звеном, существенно ослабляющим всю общегосударственную политику национальной безопасности. Индустриально развитые государства современного мира в настоящее время, на основе инновационных информационно–коммуникационных технологий, приступили к качественному преобразованию всех основных сфер общественной жизнедеятельности: от экономики до здравоохранения и тому подобное.

На данное обстоятельство особо обращается внимание в вышеназванной Государственной программе. Так, в данном документе подчеркнуто, что «одним из вызовов, на который должна ответить Российская Федерация, является переход развитых стран к формированию новой технологической базы экономических систем, основанной на использовании новейших достижений в области информатики, в том числе в здравоохранении и других сферах. Ответ на этот вызов – инновационный сценарий, направленный на формирование новой экономики, или экономики знаний и высоких технологий, в число ведущих

отраслей которой входят отрасли связи и информационных технологий. В отношении отрасли информационных технологий определены такие цели, как повышение качества жизни граждан, развитие экономической, социально-политической и культурной сфер жизни общества, а также совершенствование системы государственного управления»[246].

Для достижения этих целей необходимо, во-первых, чтобы технологическое направление политики информационной безопасности было ориентировано на формирование современной информационно-телекоммуникационной инфраструктуры, обеспечение высокого уровня ее доступности, предоставление на ее основе качественных услуг.

Следствием такой технологической политики должно оказаться обеспечение конкурентоспособности и технологического развития российских информационных технологий как на внутреннем, так и мировом рынках и киберпространствах.

Во-вторых, политика, направленная на всемерное развитие информационной сферы, при всей ее важности, не должна оказаться самоцелью. Успешная реализация такой политики должна привести к повышению качества образования, медицинского обслуживания, социальной защиты населения, содействовать развитию культуры и средств массовой информации на основе информационных технологий.

В-третьих, важным результатом политики обеспечения информационной безопасности, которого необходимо достичь в процессе реализации «Государственной программы Российской Федерации «Информационное общество (2011 – 2020 гг.)», следует рассматривать повышение эффективности государственного управления и местного самоуправления, взаимодействия гражданского общества и коммерческих организаций с органами государственной власти.

В-четвертых, в рамках политики информационной безопасности как важной

[246] Распоряжение Правительства РФ от 20.10.2010 № 1815-р (ред. От 15.08.2012) «О государственной программе Российской Федерации «Информационное общество (2011–2020 годы)». Гл. 2 // www.consultant.ru (дата обращения: 04.05.2013)

составной части политики обеспечения национальной безопасности, необходимо осуществить комплекс специальных мер. Эти меры должны быть направлены на противодействие использования информационных технологий вразрез национальным интересам России. Такой подход следует рассматривать как одно из направлений обеспечения информационного суверенитета нашей страны.

Для достижения последней из указанных целей, в рамках изучаемой Государственной программы, предусмотрена особая подпрограмма «Безопасность в информационном обществе».

«Мероприятия этой подпрограммы обеспечивают решение задачи предупреждения угроз, возникающих в информационном обществе, посредством выполнения функции государственного контроля (надзора) в сфере реализации Программы, создания средств защиты информации, мониторинга угроз, регулярной оценки защищенности компонентов инфраструктуры, ликвидации неблагоприятных последствий нарушений ее защиты, своевременной модернизации систем защиты компонентов инфраструктуры»[247].

3.3. Основные факторы влияния политики информационной безопасности на состояние национальной безопасности современной России

В условиях становления российского и формирования глобального информационного общества возрастает влияние политики информационной безопасности на состояние сферы национальной безопасности Российской Федерации. Факторы, определяющие данное влияние, следует разделить по результатам оказываемого воздействия на две основные группы.

Первая группа – это факторы, которые связаны с возникновением потенциальных (или реальных) угроз в информационном пространстве или в других областях общественной жизни, где присутствует информационная

[247] Распоряжение Правительства РФ от 20.10.2010 № 1815-р (ред. от 15.08.2012) «О государственной программе Российской Федерации «Информационное общество (2011–2020 г.)». Гл. 3 // www.consultant.ru. (дата обращения: 04.05.2013)

составляющая. Эти факторы представляют собой реакцию на явления и процессы, которые имеют явно выраженный негативный характер по своему воздействию на национальную безопасность. Политика информационной безопасности в данном случае направлена, прежде всего, на недопущение возникновения соответствующих опасностей либо на парирование или на ликвидацию угроз, если они все-таки появились.

Вторая группа факторов влияния политики информационной безопасности на состояние национальной безопасности Российской Федерации в наше время ориентирована на стимулирование процессов, имеющих позитивную природу. Правильная политика информационной безопасности позволяет более эффективно осуществлять обеспечение национальной безопасности российского государства в целом. С одной стороны, такая политика укрепляет состояние сферы информационной безопасности. С другой стороны, современные информационно-коммуникационные технологии успешно применяются для укрепления других принципиально важных сфер национальной безопасности: таких, как военная и политическая, экономическая и энергетическая, экологическая и демографическая безопасность и тому подобное.

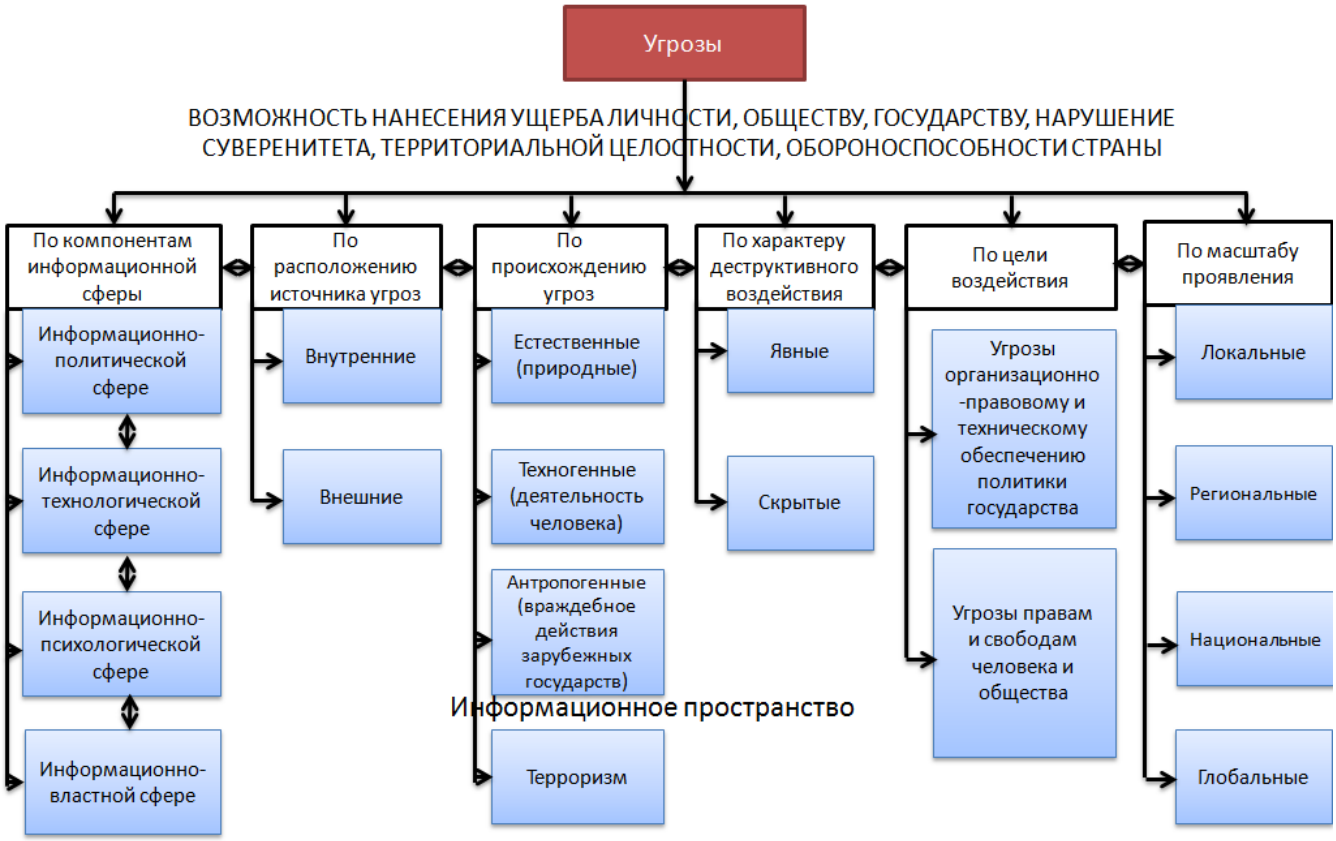
Рассмотрим более подробно первую группу факторов. Они проявляются в тех условиях и обстоятельствах, когда существуют явные (или скрытые) угрозы обеспечения национальной безопасности. Эти угрозы имеют место не только в информационной области, но и в ряде других сфер национальной безопасности, имеющих решающее значение для процесса ее обеспечения.

Данные угрозы носят, прежде всего, трансграничный характер. Они во многом связаны со сферой международных отношений, поэтому им уделено пристальное внимание в Концепции внешней политики Российской Федерации (редакция 2013 г.).

Документ содержит положения, согласно, которым, Россия «будет принимать необходимые меры в интересах обеспечения национальной и международной информационной безопасности, предотвращения угроз политической, экономической и общественной безопасности государства,

возникающих в информационном пространстве, для борьбы с терроризмом и с иными криминальными угрозами в сфере применения информационно-коммуникационных технологий, противодействовать их использованию в военно-политических целях, противоречащих международному праву, включая действия, направленные на вмешательство во внутренние дела, а также представляющие угрозу международному миру, безопасности и стабильности»[248].

Таким образом, меры по предотвращению угроз возникающих в информационном пространстве выступают в качестве важных факторов для обеспечения национальной и международной безопасности. Проведем более детальный анализ этих факторов. В ходе такого анализа в первую очередь целесообразно рассмотреть национальные интересы Российской Федерации в контексте угроз нашей национальной безопасности, приходящих из глобального информационного пространства (Рисунок 7).



[248] Концепция внешней политики Российской Федерации. Утверждена Президентом Российской Федерации В. В. Путиным 12 февраля 2013 г. Гл. 3. Ст. 32. URL: http://www.ln.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c 325787a0034c255/c32577ca0017434944257b160051bf7f. (дата обращения: 14.09.2013)

Рисунок 7 – Типология угроз национальной безопасности в глобальном информационном пространстве

Как уже отмечалось, национальные интересы представляют собой систему внутренних и внешних потребностей. Реализация этих потребностей обеспечивает нашей стране защищенность сегодня и дальнейшие определенные перспективы устойчивого развития на личном, общественном и государственном уровнях.

Такая же необходимость в защищенности и в устойчивости развития существует и для информационной сферы, что следует учитывать при изучении проблем обеспечения информационной безопасности нашей страны с учетом российских национальных интересов в этой области.

На основе этих интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности. В Доктрине информационной безопасности Российской Федерации выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает соблюдение конституционных прав, свобод человека и гражданина в области получения информации, а также пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая – включает в себя информационное обеспечение государственной политики страны, ее официальную позицию по социально значимым событиям российской и международной жизни и обеспечение доступа граждан к открытым государственным информационным ресурсам.

Третья – включает развитие современных информационных технологий, отечественной индустрии информации, в том числе средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее

продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Четвертая – включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем – как уже развернутых, так и создаваемых на территории России[249].

Все указанные в Доктрине информационной безопасности Российской Федерации четыре составляющие национальных интересов являются актуальными и в наши дни. Однако, с момента подготовки и вступления в силу Доктрины прошло почти полтора десятка лет, которые ознаменовались большими изменениями как во внутренней жизни нашей страны, так и в глобальном развитии.

Особенно революционными как в технологическом, так и в политическом планах такие трансформации оказались в информационной сфере. В связи с этим, национальные интересы Российской Федерации, сформулированные в рассматриваемом документе, требуют более глубокого осмысления – с тем, чтобы использовать их в качестве эффективного фактора развития, как информационной безопасности, так и всей системы обеспечения национальной безопасности России.

В соответствии с темой нашего исследования, особый интерес представляют первая и вторая составляющая национальных интересов из четырех указанных в обсуждаемом документе.

Первая составляющая ориентирует национальные интересы, как уже отмечалось, на область получения информации и пользования ею. Предполагается, что за последние полтора – два десятилетия произошли радикальные изменения самого информационного пространства. В настоящее время данное пространство не просто используется для доступа к определенной

[249] Доктрина информационной безопасности Российской Федерации. / Утверждена Президентом РФ 9 сентября 2000 г. № Пр-1895. Гл. 1. Ст. 1 // Российская газета. 2000. 10 сентября. № 187.

информации: оно превратилось в информационное поле, которое используется для обеспечения процессов жизнедеятельности во всех основных сферах общества. (Следует отметить, что современное информационное пространство, в первую очередь, представлено сетью Интернет).

Не обошла указанная тенденция, кончено, и политическую сферу. Информационно-коммуникационные технологии все шире используются для повышения эффективности государственного управления. Таким образом, Интернет превратился в важный коммуникационный ресурс властно-управленческого процесса.

В связи с этим И. А. Бронников пишет: «Трансформация политической коммуникации в сети Интернет основывается на следующих постулатах: происходит модификация общественно-политической системы общества, все больше политическая активность из мира реального транслируется в мир виртуальный и обратно; под воздействием нового информационного общества модифицируется политическое участие граждан, что непосредственно связано с использованием деятельности «электронных правительств» и «электронной демократии», трансформируются формы государственного управления, что ведет к «опубличиванию» политики и, наконец, тенденции мировых политиков к нарастающему использованию Интернет-технологий приводят к вовлечению большего числа граждан в политическую сферу»[250].

Тенденция к возрастанию степени публичности современной политики вынуждает участников политических процессов активно использовать пиар-технологии. Данные технологии позволяют достаточно широко осуществлять воздействие на массовое сознание как в завуалированной, так и в открытой формах. Такой подход позволяет достаточно эффективно влиять на поведение людей в масштабах отдельного региона (или даже страны), а в исключительных случаях – и в мировом масштабе.

Придать подобным политическим пиар-кампаниям широкий размах позволило использование возможностей Интернета. Таким образом, в последнее

[250] Бронников И. А. Интернет как ресурс политической власти // Право и политика. 2011. № 6. С. 1015.

время, данная сеть постепенно превратилась в важный политический ресурс влияния на общественное сознание. Этому способствовали следующие особенности Интернета как средства коммуникации.

Во-первых, данная сеть обладает всемирным масштабом охвата миллиардов пользователей, а также очень высокой скоростью распространения информации, в том числе и политических новостей. Данные обстоятельства делают Интернет чрезвычайно оперативным коммуникационным ресурсом.

Во-вторых, Интернет представляет собой мультимедийную систему, в которой осуществляется взаимодействие визуальных картин и аудиоэффектов. Применение современных технических и программных средств позволяет сочетать видео и фото, текст и звук, фото и графику в одном цифровом формате.

Таким образом, рассматриваемая сеть объединяет основные функции традиционных информационно-коммуникационных систем: радио и телевидения, телефонии и печатных изданий.

В-третьих, «всемирная паутина» обладает очень важным свойством, необходимым для использования в политической процессах: с целью их организации, управления и активизации интерактивностью. Использование принципа интерактивности позволяет организовать информационный обмен между различными пользователями Интернета.

Это позволяет создавать на основе Интернета социальные сети, которые становятся базами для организации политических акций и кампаний. Эти кампании могут инициировать как протестные и разрушительные действия, так и выступления в поддержку тех (или иных) политических деятелей и сил, что способствует стабилизации политической ситуации. Специалисты обозначают данные политические процессы в информационно-коммуникационной сфере, как псевдопубличность.

При анализе Интернета как важного ресурса современных политических процессов интересное мнение высказывает А. И. Ерина: «Интернет создал нового человека, homo scepticus, который способен анализировать информацию, подаваемую СМИ. Этот новый человек политически активен, образован. Его

онлайн-деятельность часто потом воплощается в офлайн-пространстве, а, следовательно, современный человек способен влиять на ход политических процессов: в частности, на принятие политических решений. Это надо учитывать и потому относиться к своему потенциальному избирателю, которого Интернет научил правилу: «Подвергай все сомнению». Интернет создал уникальную базу непосредственного общения политических игроков и их целевых групп, открыл достаточно широкий доступ к деятельности тех, за кого, по сути, мы идем голосовать»[251].

В то же время, виртуализация политических процессов, наряду с расширением возможностей современной политической жизни, несет и ряд опасностей и гроз для политической стабильности, а также устойчивого политического развития, затрагивая как состояние информационной безопасности, так и обеспечение национальной безопасности в целом.

Так, виртуализация политической деятельности ведет к возникновению разрыва между виртуальной и реальной политической жизнью.

Действительные насущные проблемы политического и общественного развития могут отдвигаться на задний план броскими и эффектными темами, созданными в виртуальном политическом мире с помощью пиар-технологий. Однако, эти темы не только не способствуют поступательному движению общества вперед, но зачастую, наоборот, порождают новые противоречия, которые не имеют реальных корней в политическом бытие, но с помощью виртуальной активности они поднимаются на поверхность, приводят к вспышкам и к обострению политической борьбы.

Интерактивность Интернета и созданного на его базе социальных сетей, которую иногда называют нелинейным способом представления информации, наряду с отмеченными ранее достоинствами, имеет и ряд существенных недостатков, которые наглядно проявляются при использовании данных сетей в обеспечении политических процессов.

---

[251] Ерина А. И. Интернет – политический ресурс воздействия на общественное мнение // Обозреватель – Observer . 2013. № 1. С. 94.

Нелинейность информационно-коммуникационных систем, как известно, позволяет пользователю участвовать в выводе информации. Такой эффект достигается путем участия во взаимодействии определенным образом со средством отображения мультимедийных данных[252].

В то же время, в случае, когда информационно-коммуникационные системы используются в политических целях, возникает вопрос об ответственности за организуемые информационные потоки, о достоверности и адекватности представляемой информации. Важно также, чтобы организация информационного поля позволяла представлять такие политические образы событий, которые были бы адекватны реальной картине политической жизни и так далее.

Российский политолог А. И. Демидов, анализируя данный феномен, отмечает: «Существуют факторы, существенно снижающие эффективность сетей как систем власти. Столь ценимое и значимое в сетях качество нелинейности лишает их четких линий зависимости, предопределяющих направление действия их участников, порождает прерывистость, квантификацию властных импульсов. Санкции здесь размыты, ответственность четко не предопределена»[253].

Проблемы общего характера, связанные с обеспечением безопасности в процессе превращения информационно-коммуникационных сетей в ресурс политической власти, имеют принципиальное значение для раскрытия темы нашего исследования. Однако, наряду с ними, существуют и более частные, но не менее важные вопросы, связанные с политико-информационным измерением национальной безопасности Российской Федерации. Одной из таких проблем, особенно остро вставших в последнее время, является компьютерный терроризм, или кибертерроризм.

---

[252] В качестве примера линейного и нелинейного способов представления информации можно рассматривать такую ситуацию, как проведение презентации. Если презентация была записана на пленку и показывается аудитории, то при этом способе донесения информации просматривающие данную презентацию не имеют возможности влиять на докладчика. В случае же живой презентации аудитория имеет возможность задавать докладчику вопросы и взаимодействовать с ним прочим образом. Это позволяет докладчику отходить от темы презентации: например, поясняя некоторые термины или более подробно освещая спорные части доклада. Таким образом, живая презентация может быть представлена как нелинейный (интерактивный) способ подачи информации // Мультимедия – Википедия // http://ru.wikipedia.org/wiki/%CC%F3%EB%FC%F2%E8%EC%E5%E4%E8%E0.

[253] Демидов А. И. Политика и виртуальная среда // Правовая политика и правовая жизнь. 2012. № 1. С. 93.

Интернет-ресурсы активно используются преступными террористическими организациями в следующих целях:

− пропаганда терроризма путем распространения террористических идей и идеологического воздействия на индивидов и социальные группы, склонные к их восприятию;

− создание и обеспечение функционирования каналов связи между различными террористическими группами и отдельными боевиками, координация действий региональных и глобальных террористических сетей;

− оповещение об угрозах проведения террористических действий, запугивание населения и давление на органы и представителей государственной власти с целью достижения политических целей, которые преследуют преступники-террористы;

− рекрутирование новых членов террористических организаций и распространение террористической активности на новые страны и регионы.

Эксперт по данной проблеме Е. Н. Пахарева подчеркивает: «Необходимость обсуждения вопросов защиты пользователей от распространения контента террористического характера в текущий момент приобретает весьма актуальный характер.

В современных условиях мы становимся свидетелями того, что возможность современных информационно-телекоммуникационных технологий, помимо прогрессивного и инновационного начала, несут в себе все возрастающий риск негативных воздействий на устои государственности и общественного согласия, сохранения нравственных ценностей и традиций Отечества. По-нашему мнению, эффективная защита интересов личности, общества и государства в этих условиях невозможна без принятия комплекса национальных и международных организационно-правовых мер»[254].

Кроме необходимости защиты пользователей системой Интернет от распространения контента террористического характера, существует еще ряд

[254] Пахарева Е. Н. Защита пользователей от распространения контента террористического характера в сети Интернет: политологический аспект проблемы // Социальная политика и социология. 2010. № 2. С. 82.

проблем ограничения права доступа к информации в целях защиты здоровья и нравственности.

Эти проблемы также непосредственно входят в поле информационного направления процесса обеспечения национальной безопасности. К таким вопросам относят следующие виды преступной деятельности в информационно-коммуникационной среде:

– проблемы, связанные с размещением порнографического контента. Это ключевой вопрос при обсуждении прав и свобод человека в информационной сфере по соображениям нравственности. Особенно следует отметить проблему детской порнографии. Сетевая детская порнография способствует вовлечению в преступную деятельность латентных педофилов и людей со слабыми морально-нравственными устоями;

– вопросы, возникающие в связи с контентом, содержащим информацию о наркотиках. Российское законодательство, в целях охраны здоровья граждан содержит всего лишь несколько норм, ограничивающих свободу слова и право доступа к информации. Это, в частности, касается информации о наркотиках. При всей нечеткости формулировок, внутренние правила интернет-сообществ также запрещают пропаганду наркотиков;

– проблемы, связанные с контентом о самоубийствах. Такие трагедии (в том числе коллективные), как показывает печальная практика, могут быть спровоцированы информацией на специальных сайтах в Интернете. Такие самоубийства получили название «киберсуицид»[255].

Рассмотренные нами проблемы, связанные с распространением в сети Интернет контента, содержащего информацию террористического, порнографического характера, пропагандирующего наркотики, самоубийства и так далее, имеют место во многих странах и, к сожалению, широко распространены в глобальном информационном пространстве.

[255] См.: Щербович А. А. Ограничения свободы слова в Интернете в целях защиты нравственности и здоровья граждан // Политика и общество. 2011. № 4. С. 126–132.

При этом эксперты по информационной безопасности отмечают проблемы, которые присущи, в первую очередь, российскому киберпространству. К таким проблемам, прежде всего, относится распространение слухов в российском сегменте сети Интернет – Рунете.

«Слухи – это специфический вид неформальной межличностной коммуникации, в процессе которой сюжет, до известной степени отражающий некоторые реальные или вымышленные события, становится достоянием обширной диффузной аудитории…

Таким образом, слухи, во-первых, – это известие, новость, сообщение, информация. Во-вторых, сообщение, недостаточно отражающее реальное положение дел или их искажающее. Если даже оно не полностью ложное, то извлечь каплю правды из него дано далеко не каждому.

В-третьих, с помощью слухов создается и передается общественное мнение, настроение, социальные стереотипы и установки аудитории, информационная ситуация в регионе. В-четвертых, они являются средством психологического воздействия (изменения мнений, отношений, настроений, поведения, удовлетворения потребностей людей и социальных групп)»[256].

Слухи получили достаточно серьезное распространение в российском сегменте Интернета. Данное явление обусловлено рядом причин. К ним можно отнести следующие причины.

Во-первых, наше общество, переживающее постсоветский период, является переходным. За последнюю четверть века произошли серьезные изменения во всех сферах жизни российского общества. Однако, не все серьезные социально-экономические проблемы получили в результате этих трансформаций свое разрешение в полной мере.

Во-вторых, в российском обществе продолжает сохраняться очень существенное социальное расслоение, нерешенность некоторых важных системных социальных вопросов. Кроме того, в постсоветский период

[256] Караяни А. И. Слухи как средство информационно-психологического противодействия // Психологический журнал. 2003 г. Т. 24. № 6. С. 25.

сформировалась относительно небольшая группа сверхбогачей, которые ведут, в информационном плане, достаточно скрытный, замкнутый образ жизни. В то же время, значительная часть населения живет за чертой бедности и вне фокуса внимания средств массовой информации и редакторов новостных программ.

Так, журналист Российской газеты В. В. Выжутович, обсуждая проблему усиления социального неравенства, пишет: «Богатые получают существенно большую часть прироста национального дохода, чем бедные. Разрыв доходов между бедными и богатыми сегодня достиг 15-кратной величины. Хотя кто-то считает, что и эта цифра занижена, поскольку не отражает скрытых доходов. Если же их учесть, то разрыв получится 20-кратным… Что ненормально. Международная практика показывает, что наилучшее самочувствие общество имеет, когда различие в доходах между 10 процентами самых богатых и 10 процентами самых бедных – от 5 до 8 раз. Если эта цифра увеличивается, у людей возникает ощущение несправедливости в распределении доходов, что ведет к росту социальной напряженности, к демотивации труда и в конце концов к дестабилизации общества»[257]. Подобная ситуация является благодатной средой для возникновения и распространения различных, подчас самых невероятных слухов.

В-третьих, в переходном обществе существенные трансформации претерпевают и средства массовой информации. Однако, существует определенная неудовлетворенность деятельностью российских СМИ как в обществе, так и среди специалистов.

Например, И. И. Новикова пишет: «Вместо того чтобы быть инструментом механизма сбалансированности интересов личности, общества и государства, СМИ становятся инструментом разрушения не только зыбкого баланса интересов, но и самого механизма балансирования в его системном виде»[258].

Подобного рода определенное недовольство тем, как многие СМИ выполняют свои функции в российском информационном пространстве,

[257] Выжутович В. Роскошь как средство передвижения // Российская газета. 2013. 12 апреля. № 80. С. 3.
[258] Новикова И. И. Стратегия информационного развития и национальной безопасности России // Власть. 2009. № 2. С. 44.

стимулирует возникновение различных суррогатов информации и, в первую очередь, слухов.

Политологический анализ показывает, что распространение слухов в сети Интернет представляет собой отнюдь не безобидную циркуляцию досужих вымыслов, а информационный процесс, который напрямую затрагивает обеспечение национальной безопасности. Слухи могут распространять не только законопослушные граждане, но и экстремисты, информационные террористы, и другие агрессивно настроенные участники информационно-коммуникационного процесса.

В таких случаях речь может идти о распространении тревожных и нервозных слухов, которые призваны сеять панику и порождать смуту.

Е. М. Куликов, обсуждая данную проблему, отмечает, что в современных условиях «приобретает важность и практическую направленность дальнейшая разработка методологических и методических аспектов проведения мониторинговых социологических исследований в сети Интернет с целью контроля над процессом генезиса и распространения слухов. В противном случае мы столкнемся с угрозой мощного информационного воздействия на население, так как сейчас слухи в Интернете распространяются во много раз быстрее, чем традиционным способом, известным с древних времен» [259].

Вторая составляющая национальных интересов Российской Федерации в информационной сфере, выделенная в Доктрине информационной безопасности Российской Федерации, как уже отмечалось ранее, непосредственно связана с информационным обеспечением государственной политики Российской Федерации. Данное обеспечение осуществляется как внутри страны, так и на международном уровне.

В последнее время в условиях становления и дальнейшего развития глобального информационного общества все большое значение приобретает информационная поддержка и сопровождение государственной политики нашей

[259] Куликов Е. М. Перспектива противодействия слухам в глобальной сети Интернет в целях обеспечения информационной безопасности // Власть. 2011. № 3. С. 68.

страны в современном мировом сообществе. Данные действия Российской Федерации приходится осуществлять в непростой международной обстановке: когда нашей стране приходится отстаивать национальные интересы в различных регионах мира.

В то же время, в глобальном информационном пространстве достаточно сильным влиянием обладают, прежде всего, Соединенные Штаты. Так, А. Д. Солодовников отмечает: «Асимметрия между Россией и США в информационной сфере не только не сокращается, но и многое говорит о том, что такое положение еще будет долго сохраняться. Отсюда возможности успешного противоборства российских СМИ и дальше будут базироваться на человеческом факторе, а именно: на профессионализме непосредственно причастных к этому полю деятельности специалистов, их адекватной рефлексии на быстротечность событий, с гуманными целями»[260].

Указанная асимметрия складывались на протяжении многих десятилетий. Во-первых, во второй половине XX – начале XXI вв. Америка сумела достичь значительного отрыва от других государств в развитии информационно-коммуникационных технологий.

Во-вторых, эта страна имеет возможность выделять значительные финансовые ресурсы для обеспечения рекламно-пропагандистских кампаний, которые проводятся в широких масштабах: вплоть до глобальных размеров.

В-третьих, в США накоплен значительный опыт функционирования различных неправительственных организаций и фондов, которые ориентированы на международную деятельность и активно участвуют в информационной поддержке внешней политики своей страны.

В-четвертых, Соединенные Штаты занимают ведущие позиции в сфере массовой информации и коммуникации. В этой стране созданы и успешно действуют крупнейшие в мире информационные агентства, глобальные спутниковые телевизионные и радиосети, печатные информационные издания,

[260] Солодовников А. Д. К вопросу о проблеме информационной безопасности контекста национальных информационных интересов // Социально-гуманитарные знания. 2011. № 2. С. 327.

распространяемые по всему миру. Не следует забывать и про то, что США постоянно стремятся сохранить фактический контроль над системой Интернет.

Такой подход, как показывает практика, позволяет Соединенным Штатам распространять свое информационное поле практически на весь мир, на те страны и регионы, где имеются их геополитические жизненно важные интересы.

Вице-президент Внешнеполитической ассоциации Н. Н. Извеков по данному поводу пишет: «Наблюдаемое ныне в мире переплетение «информационных полей» разных стран таит в себе как большие коммуникационные возможности, так и немалые опасности, которые связаны с разной политико-идеологической направленностью потоков информации. Иногда такие различия достигают степени открытого антагонизма, порождающего риски возникновения информационно-психологических кампаний или противоборства, которое может балансировать на грани возникновения вооруженного конфликта между отдельными странами»[261].

Необходимо отметить, что Соединенные Штаты ведут пропагандистскую деятельность в глобальном информационном пространстве как самостоятельно, так и во взаимодействии со своими союзниками. Наибольшее внимание со стороны нашего государства заслуживает активность блока НАТО на российском направлении мирового информационно пространства.

В этой организации еще в 2001 году было сформировано Управление общественной дипломатии. Принципы и основные направления деятельности этой структуры проанализированы А. Д. Рогозиным. Автор пришел к следующему выводу: «Обобщая, можно говорить о том, что общественная дипломатия НАТО, которая в случае обострения двусторонних отношений может представлять вполне реальную угрозу информационной безопасности РФ, в настоящее время не направлена против России. Требуя от структур и официальных лиц НАТО соблюдения этой информационной политики, Россия,

[261] Извеков Н. Н. Факторы, формирующие образ страны в окружающем мире // / Обозреватель – Observer. 2010. № 1. С. 58.

тем не менее, заинтересована в развитии сотрудничества с Североатлантическим альянсом – так же, как и сам альянс»[262].

В то же время, не избегая партнерских отношений с США и НАТО в информационной сфере, наша страна должна проводить целенаправленную работу по защите информационной безопасности как составной части национальной безопасности, принимая в расчет сложившуюся асимметрию между Россией и США в информационном пространстве. Возможно, следует искать асимметричные ответы на потенциальные информационные угрозы (Рисунок 8).

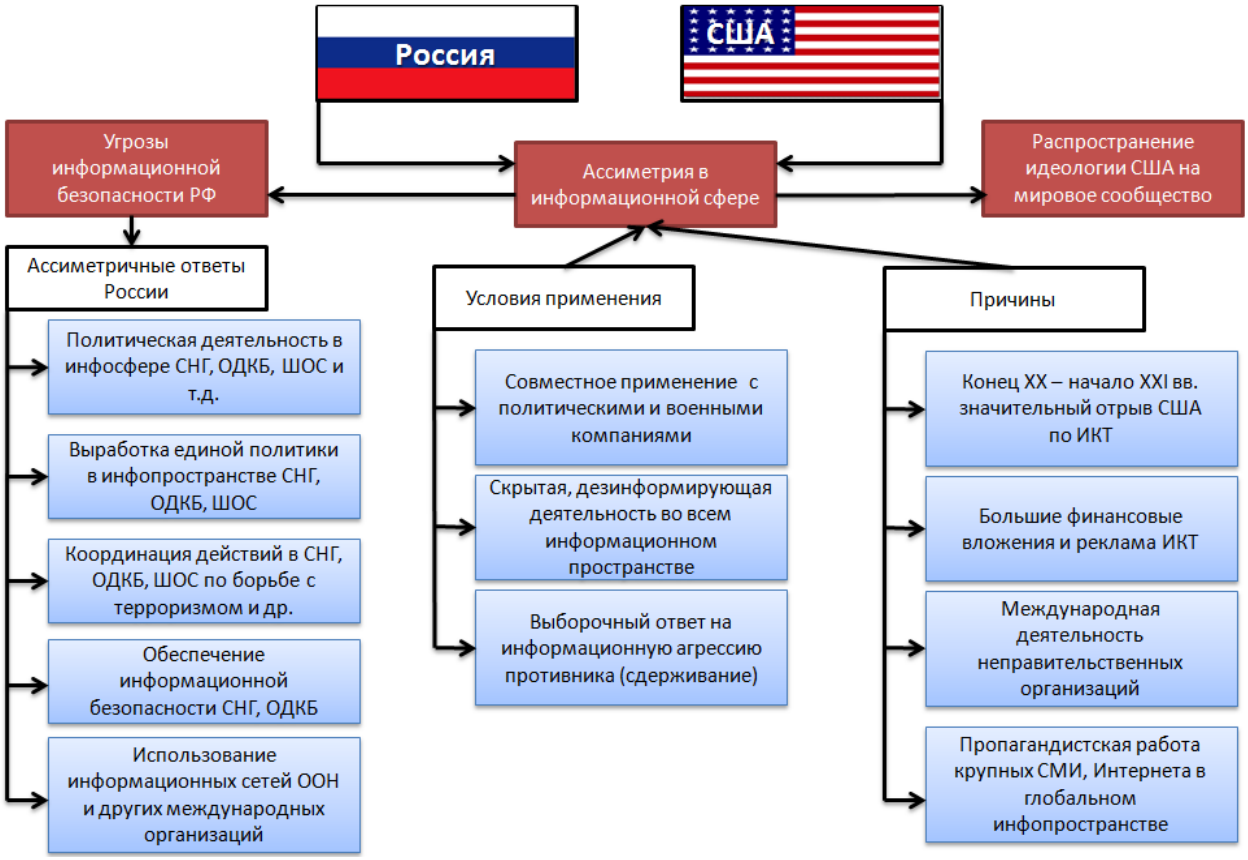


Рисунок 8 – Асимметрия отношений России и США в информационной сфере

Прежде всего, следует сосредоточить активность в информационном пространстве тех регионов, где особенно важны наши национальные интересы. Речь, в первую очередь, идет о государствах – членах ОДКБ и СНГ.

[262] Рогозин А. Д. «Общественная дипломатия» НАТО: информационная безопасность России // Власть. 2008. № 9. С. 32.

Расширение сотрудничества по обеспечению информационной безопасности является перспективным направлением активизации деятельности ОДКБ в сфере защиты национальной и международной региональной безопасности. Данную точку зрения разделяют и многие эксперты в данной области. Так, В. Струговец пишет: «Анализ сложившейся ситуации в информационной сфере позволяет выделить ряд перспективных направлений сотрудничества государств – членов ОДКБ в рамках обеспечения международной информационной безопасности: содействие выработке международного законодательства, соглашений и договоренностей, противодействующих угрозам в информационной сфере; определение и характеристика угроз, связанных с незаконной деятельностью в информационной сфере, вмешательством в информационные системы государств – членов ОДКБ; достижение общего понимания опасности потенциальных и реальных угроз в информационной сфере»[263].

В «Концепции формирования информационного пространства СНГ»[264], принятой в 1996 году решением Совета Глав Правительств, при определении национальных и общих интересов в деле развития сотрудничества в информационной сфере и в организации деятельности по формированию информационного пространства государств – членов Содружества было указано на обеспечение информационной безопасности, как важнейшего элемента обеспечения коллективной безопасности стран Содружества.

В «Доктрине информационной безопасности Российской Федерации» подчеркивается: «При осуществлении международного сотрудничества Российской Федерации в области обеспечения информационной безопасности особое внимание должно уделяться проблемам взаимодействия с государствами – участниками Содружества Независимых Государств»[265].

---

[263] Струговец В. Перспективные направления информационной политики ОДКБ // Власть. 2011. № 8. С. 98

[264] Концепция формирования информационного пространства СНГ [Электронный ресурс] / Утверждено решением СГП СНГ от 18 октября 1996 г. – Режим доступа: http://www.zakonprost.ru/content/base/41929. (дата обращения: 17.02.2013)

[265] Доктрина информационной безопасности Российской Федерации. / Утверждена Президентом РФ 09 сентября 2000 г. № Пр-1895. Гл. 3. Ст. 7 // Российская газета. 2000. 10 сентября. № 187.

Опыт сотрудничества России по формированию и реализации политики информационной безопасности в Евразийском регионе насчитывает уже почти два десятилетия и будет более подробно рассмотрен в параграфе 5.1 данного исследования.

* * *

Важно подчеркнуть, подводя итоги изложенного в данной главе, что, во-первых, для оценки состояния национальной безопасности прежде всего важен процесс мониторинга этого феномена. Для этого используют критерии и показатели оценки состояния национальной безопасности, которые представляют собой признаки, на основании которых производится оценка, состояние всей этой сферы в целом.

Данная оценка опирается на определенные показатели, которые имеют как количественный, так и качественный характеры. Таким образом, важно подчеркнуть, что сущность и состояние национальной безопасности раскрывается в системе, состоящей из ее критериев и показателей.

Во-вторых, при анализе концептуальных основ политики национальной безопасности следует отметить, что одной из центральных категорий выступает понятие «угроза национальной безопасности». В зависимости от характера опасности и источника причинения ущерба, выделяют три основные группы угроз национальной безопасности: естественно-природные, техносферные и антропогенные.

На первый план в современной международной политике выходят новые вызовы и угрозы, имеющие трансграничную природу. Среди них по масштабам проявления, степени диверсификации, возможному ущербу и последствиям выделяется угроза информационной безопасности.

В-третьих, особое значение имеет информационная компонента в средствах обеспечения национальной безопасности, и ее удельный вес в этом процессе будет возрастать. Значительная часть сил обеспечения национальной

безопасности также ориентирована на решение стратегических задач, непосредственно (или косвенным образом) связанных с решением задач по обеспечению информационной безопасности.

Для управления и координации действий указанных сил и использования названных средств в информационной области в нашей стране проводится соответствующая политика. В структуре этой политики следует выделить два основных направления: государственно-правовое и технологическое.

Однако, в условиях развития информационного общества в нашей стране и достижения процессов информатизации глобальных масштабов становится все более очевидным, что обеспечить информационную безопасность путем деятельности органов государственной власти, правоохранительных структур, а также развития законодательной и нормативно-правовой баз достаточно затруднительно. Полностью не решает эту проблему даже применение инновационных технических средств.

В современном мире прилагаются значительные усилия для формирования глобальной культуры кибербезопасности. Это свидетельствует о том, что обеспечение информационной безопасности превратилось в актуальную глобальную проблему наших дней. Анализ основных элементов, необходимых для формирования культуры информационной безопасности, показывает, что в них достаточно ярко выражен политический аспект.

В рамках политики информационной безопасности как важной составной части политики обеспечения национальной безопасности, следует предусмотреть комплекс специальных мер, которые должны быть направлены на противодействие использования информационных технологий вразрез национальным интересам России.

В-четвертых, правильная политика информационной безопасности позволяет более эффективно осуществлять обеспечение национальной безопасности российского государства в целом. Меры по предотвращению угроз, возникающих в информационном пространстве, выступают в качестве важных факторов для обеспечения национальной и международной безопасности.

Такой подход особенно важен, потому что сеть Интернет постепенно превратилась в важный политический ресурс влияния на общественное сознание. Этому способствовали следующие особенности Интернета как средства коммуникации: всемирный масштаб охвата, очень высокая скорость распространения политической информации, мультимедийность и интерактивность.

Интернет-ресурсы активно используются в преступных целях: кибертерроризм, размещение порнографического контента или контента, содержащего информацию о наркотиках, или сведения о самоубийствах («киберсуицид»). Российскому информационному пространству присуща проблема распространения слухов, которая потенциально несет угрозу мощного информационного воздействия на население.

В-пятых, в отношениях России с США и НАТО в информационной сфере сложилась асимметрия, которая не только не сокращается, но и еще, возможно, будет долго сохраняться. В данных условиях нашей стране следует искать асимметричные ответы на потенциальные информационные угрозы с Запада. Следует сосредоточить активность в информационном пространстве тех регионов, где особенно важны наши национальные интересы. (СНГ, ОДКБ, ЕврАзЭС и ШОС).

4. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ В УСЛОВИЯХ СОВРЕМЕННЫХ МЕЖДУНАРОДНЫХ ПРОЦЕССОВ

В наше время при исследованиях вопросов обеспечения национальной, в том числе и информационной безопасности Российской Федерации все чаще внимание обращается на изучение роли и места политических факторов в этом процессе. Особое место среди них в начале XXI столетия стал занимать фактор мировой политики. Действие этого фактора в значительной мере обуславливается процессом глобализации современного мира.

Изучение международно-политической составляющей информационной безопасности позволяет более полно учитывать взаимодействие России с ведущими мировыми державами и сопредельными странами в глобальном информационном пространстве. В то же время, при защите национальных интересов и безопасности России в современных условиях постоянно необходимо учитывать роль глобального информационного противоборства в данном процессе. Такая ситуация требует специального изучения, поскольку существенным образом влияет на изменение ситуации в глобальном информационном сообществе при обеспечении национальной безопасности нашей страны.

Все большое значение также информационная безопасность приобретает для геополитики современной России. Данный феномен требует проведения развернутого геополитического анализа. Цель такого анализа – осмысление особенностей обеспечения безопасности нашей страны в глобальном информационном пространстве второго десятилетия XXI столетия.

Данный анализ важен также для разработки и реализации политики национальной безопасности России в современном мире, где в результате научно-технического прогресса формируется общество XXI века. В «Окинавской Хартии глобального информационного общества», принятой при участии нашей страны на Саммите Группы восьми в 2000 году, записано: «Информационно-

коммуникационные технологии (IT) являются одним из наиболее важных факторов, влияющих на формирование общества XXI века. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. IT быстро становятся жизненно важным стимулом развития мировой экономики»[266].

Под революционным воздействием информационно-коммуникационных технологий изменяются важнейшие геополитические характеристики современных государств, а также мирового и регионального геополитических пространств. Данные изменения привели к формированию глобального геополитического пространства, которое следует рассматривать и как геополитический феномен мирового масштаба.

Государственные границы государств стали прозрачными в информационном измерении. Возникли такие ранее не известные в международных отношениях явления, как глобальное информационное противоборство, информационная агрессия и информационная война.

4.1. Международные аспекты информационной безопасности Российской Федерации

Современная ситуация в мире характеризуется высокой динамикой международных политических процессов как на глобальном, так и на региональном уровнях. Для мирового политического развития, как отмечают специалисты, характерны два основных тренда: упорядочивание и хаотизация.

Тренд упорядочивания (структуризации, регуляции, управления) процессов мирового политического развития проявляется в создании различных формальных и неформальных структур: международных организаций, различных межгосударственных «клубов» (Группы восьми, Группы двадцати), межгосударственных коалиций, союзов, форумов, включающих государственные

[266] «Окинавская Хартия глобального информационного общества», (Окинава, 22 июля 2000 г.). URL: http://www.iis.ru/library/okinawa/charter.ru.html. (дата обращения: 19.11.2013)

и негосударственные структуры (Давосский форум, Петербургский экономический форум и тому подобное).

Хаотизация же прослеживается в таких процессах, как распад союзов и коалиций (например, ОВД), очевидное несоблюдение международных норм, договоров и тому подобное, появление новых феноменов, природа которых плохо согласуется с тем, что было ранее, и так далее.[267]

В наши дни достаточно наглядно проявляются международные политические процессы, отражающие хаотизацию и затрудняющие предвидение перспектив мирового развития. Тренд хаотизации служит индикатором деструктивных явлений, непосредственно оказывающих негативное влияние на фундамент политической организации международного сообщества.

В данной связи Министр иностранных дел Российской Федерации С. В. Лавров отмечает: «В целом, очевидно, что мир переживает беспрецедентный, по историческим меркам, переходный период, сопровождающийся перелицовкой геополитического ландшафта, формированием новой расстановки сил»[268].

В таких условиях в некоторой степени увеличивается уровень неопределенности траекторий мирового политического развития, формируются предпосылки для существенной трансформации всей мировой социально-политической структуры и, соответственно, – принципов обеспечения международной безопасности. Такие политические изменения глобального масштаба сочетаются с революционными и не менее значимыми сдвигами в науке и технике.

Научно-технический прогресс расширяет сферы деятельности для акторов мировой политики, предоставляет им новые инструменты воздействия на членов мирового сообщества, международные политические институты и процессы. Повышение политической активности в результате внедрения научно-

---

[267] См.: Метаморфозы мировой политики / под общ. Ред. М. М. Лебедевой. М.: МГИМО-Университет, 2012. С. 10.

[268] Лавров С. В. Пресс-конференция Министра иностранных дел России, посвященная итогам деятельности российской дипломатии в 2012 г. // Международная жизнь. 2013. Февраль. С. 2.

технических инноваций также способствует понижению политической организации структуризации мирового сообщества.

«Современный скачок в научно-техническом развитии повлиял, прежде всего, на развитие тренда хаотизации. В результате НТР слабый актор оказался сильным в смысле возможного нанесения значительного ущерба другим, что во многом сломало прежние структуры в сфере безопасности. Кроме того, новые коммуникационные и информационные технологии принципиальным образом расширили взаимодействие негосударственных акторов, вывели его на глобальный уровень в совершенно иных масштабах»[269].

Таким образом, новый этап научно-технической революции, связанный с развитием информационно-коммуникационных технологий, непосредственно оказывает влияние на основные тенденции эволюции современных международных отношений, а также структуру и особенности деятельности участвующих в этих отношениях акторов. Научно-технический прогресс привел к становлению глобального информационного общества, которое представляет собой новый этап развития цивилизации.

На этом этапе ведущей сферой человеческой жизнедеятельности становится информационное пространство, которое развивается до глобальных масштабов, а важнейшими продуктами производства и обмена выступают знания и информация.

Субъекты глобального информационного общества часто выступают в качестве акторов международных отношений и наоборот: акторы международных отношений становятся непосредственными и деятельными участниками глобального информационного общества.

В данной связи следует отметить, что понятия «акторы современных международных отношений» и «субъекты глобального информационного общества» достаточно близки по характеру и природе своей деятельности. Основное отличие заключается в том, что акторы современных международных

[269] См.: Метаморфозы мировой политики / под общ. Ред. М. М. Лебедевой. М.: МГИМО-Университет, 2012. С. 17–18.

отношений действуют в реальном геополитическом пространстве, а субъекты глобального информационного общества – в виртуальном глобальном информационном пространстве.

А. В. Гуменский выделяет шесть основных групп участников современного глобального информационного общества: государства, крупный бизнес, транснациональные медиакорпорации, гражданские институты, некоммерческие и неправительственные организации, транснациональные социальные сети, индивидуумы[270]. Российский исследователь справедливо выделяет государства в качестве первостепенных участников глобального информационного общества.

Такая оценка обусловлена следующими причинами. Во-первых, современные государства выступают в качестве главных инициаторов и участников политической коммуникации, которая оказывает влияние на общественное мнение и мировую политику. Во-вторых, в наши дни государства обладают или контролируют огромные материальные и человеческие ресурсы, что дает им значительное преимущество перед другими участниками глобального информационного общества и акторами международных отношений.

В распоряжении государства находятся также мощный аппарат управления и силовые структуры для обеспечения национальной безопасности.

В-третьих, государство является первичным субъектом современного международного права. В результате двухсторонних и многосторонних межгосударственных договоров формируются нормы и принципы поведения субъектов международных отношений и глобального информационного общества.

Большие интересы в глобальном информационном обществе имеет другой его ведущий участник – крупный бизнес. В последние годы особенно усилилось влияние на международные процессы глобальной финансовой системы, основу которой составляют банки и офшоры.

---

[270] Гуменский А. В. Управление международной информацией // Международные процессы. 2010. № 1. Т. С. 33.

Так, И. В. Красавин пишет: «Современная международная система характеризуется повышенным влиянием финансовых организаций на институциональное управление политикой и экономикой на глобальном и национальном уровнях. Характерной чертой отношений финансовой системы с остальными международными акторами является ее негосударственный, частный или корпоративный характер.

В отношениях с финансовыми организациями национальные государства не являются привилегированными и конкурируют за капитал так же, как и прочие деловые и бюрократические организации. Такая система отличается от предыдущей, Бреттон-Вудской, в которой международные финансы располагались в сфере межгосударственных отношений»[271].

Таким же образом негосударственные финансовые организации и другие структуры крупного бизнеса оказывают воздействие на процесс формирования глобального информационного общества. Эти структуры проводят прямую и скрытую рекламу своих интересов, осуществляют инвестирование в СМИ глобального, регионального и местного уровня, в том числе и в зарубежных странах.

Можно сказать, что в процессе формирования глобального информационного общества государства и крупный бизнес так же, без каких-либо привилегий, конкурируют за информационные ресурсы вместе с другими участниками этого процесса. Данная ситуация во многом аналогична упомянутому выше феномену конкуренции за капитал в глобальной финансовой системе.

Большую роль в глобальном информационном обществе играют транснациональные медиакорпорации. Эти корпорации создают и контролируют большие потоки информации, которые представляют собой глобальные и региональные стратегически информационные магистрали. Вокруг этих

[271] Красавин И. В. Глобальная финансовая система в мировой политике: банки и оффшоры // Негосударственные участники мировой политики./ Под ред. М. М. Лебедевой, М. В. Харкевича. М.: Аспект Пресс. 2013. С. 20.

магистралей происходит структурирование глобального информационного пространства.

В данной связи В. В. Фокина пишет, что «роль организатора информационных потоков, несомненно, принадлежит СМИ. Этому способствует возможность мгновенной передачи информации на большие расстояния рассредоточенной в глобальном пространстве массовой аудитории. При этом нередко СМИ принадлежит не только роль передатчика информации, но и ее создателя»[272].

Среди значимых участников глобального информационного общества следует также выделить гражданские институты, некоммерческие и неправительственные организации (НКО). Данные организации распространяют в глобальном информационном пространстве идеи, связанные с общечеловеческими ценностями и гуманистическими принципами, используя в первую очередь сеть Интернет.

Серьезным недостатком в деятельности этих организаций следует рассматривать зависимость от внешних источников финансирования. Например, как показали проверки таких организаций в России в начале 2013 года, около 600 зарегистрированных в России НКО получают значительное финансирование из-за рубежа.

Данное финансирование частично осуществляется даже по дипломатическим каналам в нарушение норм международного права. Наличие серьезной финансовой зависимости НКО от властных структур зарубежных государств вызывает в российском обществе небезосновательные подозрения в их политической ангажированности и необъективности.

Все более значимым субъектом глобального информационного общества в наши дни становятся трансграничные социальные сети. В отличие от гражданских институтов, некоммерческих и неправительственных организаций они представляют собой неформальные структуры, так как не имеют юридического статуса.

---

[272] Фокина В. В. СМИ как акторы мировой политики / Вестник МГИМО-Университета. 2013. № 1 (28). С. 61.

Как любые неформальные институты, данные сети отличаются гибкостью и мобильностью в своей деятельности. Они свободны от бюрократических процедур и формальных ограничений. Социальные сети обладают в глобальном информационном пространстве практически такими же возможностями, как и другие его участники, включая государства, крупный бизнес и тому подобное. В то же время, социальные сети могут осуществлять свою деятельность в завуалированной форме, быстро приспосабливаясь к изменяющимся политическим и социальным условиями.

Возрастание роли социальных сетей в информационном пространстве отражает более общую тенденцию глобального развития – переход к информационно-сетевому принципу организации общества.

Так, А. П. Кочетков, рассматривая данный вопрос, отмечает: «Ведущей тенденцией организации общества постепенно становится информационно-сетевой принцип, который предполагает, что основной социальной ячейкой является сеть, некое объединение граждан, близких по духу и интересам. Все общество будет представлять собой систему сетевых структур, а правящим классом в таком обществе становится новая социальная группа – нетократия, формируемая из представителей транснациональных корпораций, каждый из которых станет куратором одной из сетей»[273].

Высокий уровень доступности и высокая скорость коммуникации в глобальном информационном пространстве создают благоприятные условия для широкого присутствия в нем даже отдельных индивидуумов. Причем в качестве этих индивидуумов выступают не профессиональные пользователи информационно-коммуникационных технологий – специалисты по PR, представители СМИ и другие производители новостей и информации, а частные граждане, имеющие доступ в Интернет.

Таким образом, к настоящему времени в мире, в результате колоссальных достижений научно-технического прогресса в области информационно-

[273] Кочетков А. П. Власть и элиты в глобальном информационном обществе // Политические исследования. 2011. № 5. С. 11.

коммуникационных технологий и под воздействием процесса глобализации, сформировалось глобальное информационное общество, жизнедеятельность которого протекает в глобальном информационном пространстве. Для стабильного и устойчивого развития данного общества необходимо обеспечение в нем информационной безопасности, которая также имеет глобальный характер.

Обратной стороной глобальной информатизации человеческого сообщества стала проблема обеспечения глобальной информационной безопасности. Российская Федерация активно представлена во всех основных группах участников глобального информационного общества. В данной связи обеспечение национальной безопасности нашей страны непосредственно связано с процессами поддержания глобальной информационной безопасности.

Исследователи проблем обеспечения информационной безопасности в современном мире отмечают, что в настоящее время имеются реальные возможности для создания угроз и нанесения ущерба безопасности мирового сообщества и отдельных его членов при помощи информационно-коммуникационных технологий.

Так, А. В. Крутских приходит к следующему выводу: «Основная озабоченность в сфере обеспечения международной информационной безопасности связана с возможностью применения информационно-коммуникационных технологий (ИКТ) в целях, не совместимых с задачами обеспечения международной стабильности и безопасности. Важнейшими угрозами здесь видятся враждебное использование ИКТ на уровне государств против информационных инфраструктур в политических, в том числе военных целях, преступная и террористическая деятельность в киберпространстве»[274].

Например, в США были проведены аналитические исследования и эксперименты под руководством Агентства информационной безопасности министерства обороны, которые показали, что степень уязвимости компьютерных систем и баз данных военного ведомства США достаточно высока. Проникнуть в

[274] Крутских А. В. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. 2007. Т. 15. № 1. С. 28.

мозговой центр Пентагона оказывается не сложно, так как он имеет множество различных выходов в другие информационные системы как внутри государства, так и за его пределами.

В настоящее время можно достаточно легко нарушить работу информационных сетей индустриально развитого государства через каналы Интернета. Здесь в качестве примера могут служить мощные запланированные атаки компьютерных хакеров на сайты ряда крупных американских компаний или правительственные сайты Эстонии сразу после демонтажа памятника «Воину-освободителю».

Было продемонстрировано хакерское превосходство над профессионалами, обеспечивающими электронную безопасность авторитетных сайтов. Следует обратить внимание, что никакого взлома серверов не было, система безопасности нигде не нарушалась, Однако, в США это впервые оценили как «кибертерроризм».

Значение сетей Интернета в развитых странах уже сейчас настолько велико, что малейшее посягательство на их неприкосновенность расценивается как жизненная угроза безопасности страны[275]. В составе военно-воздушных сил США даже было образовано новое Киберкомандование, под руководством которого будут создаваться, тренироваться и снаряжаться силы для проведения длительных глобальных операций в киберпространстве и посредством киберпространства, полностью интегрированных с воздушными и космическими операциями[276].

Доступность глобальной компьютерной сети позволяет передавать необходимую информацию в любой регион мира и выполнять многие задачи, связанные с информационным противоборством. Не исключено, что в рамках информационного противоборства, самостоятельное развитие может получить кибернетическая борьба, в ходе которой будут наноситься мощные

---

[275] Ноговицын А. А., Барвиненко В. В., Мушков Ю. И. Методика оценки и пути обеспечения военной безопасности государства // Вестник Академии военных наук. 2004. № 1(6). С. 115.

[276] Пентагон борется с виртуальными врагами. Электрон. дан. [Б.м., 2007]. Режим доступа: http://www.newsru.com/world/19sep2007/kiber.html. (дата обращения: 13.03.2014)

информационные удары по интегрированным компьютерным системам противника.

В данной связи в «Доктрине информационной безопасности Российской Федерации» дан анализ угроз информационной безопасности нашей страны. «По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

− угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

− угрозы информационному обеспечению государственной политики Российской Федерации;

− угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

− угрозы безопасности информационных и телекоммуникационных средств и систем: как уже развернутых, так и создаваемых на территории России»[277].

Все вышеуказанные виды угроз информационной безопасности Российской Федерации имеют значительное международное измерение и в достаточно большой степени связаны с факторами и процессами, находящимися за пределами нашей страны. Рассмотрим данную международную составляющую угроз информационной безопасности более подробно.

Так, среди «угроз конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности» наиболее серьезной представляется опасность «вытеснения российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и

[277] Доктрина информационной безопасности Российской Федерации // URL: http://www.rg.ru/OFICIAL/DOC/MIN_AND_VEDOM/MIM_BEZOP/DOCTR.SHTM. (дата обращения: 27.09.2013)

политической сфер общественной жизни России от зарубежных информационных структур»[278]. Данная угроза может реализовываться по нескольким направлениям.

Первое направление связано с деятельностью СМИ ведущих стран Запада, которые, в данный момент, контролируют большую часть глобального информационного пространства. Им принадлежат (или находятся под их контролем) крупнейшие международные информационные агентства и службы новостей, глобальные телевизионные компании и информационные сети в Интернет.

Как показывает практика, освещение многих основных событий международной жизни и особенно конфликтов, затрагивающих национальные и геополитические интересы ведущих держав, освещается в СМИ стран Запада и нашей страны с разных позиций; при этом даются разные идентификации «своих» и «чужих» в мировых политических процессах.

В последние десятилетия западные СМИ теснят в мировом информационном пространстве медийные структуры из некоторых других регионов современного мира. Наиболее ярким примером в этом плане является вхождение в глобальное информационное пространство катарского телевизионного канала «Аль-Джазира».

«Уже в конце 1990-х годов «Аль-Джазира», следуя провозглашенным ею принципам независимости, предъявила своей аудитории аналитические материалы, которые зачастую противоречили западной трактовке событий в регионе (имеется в виду Арабский Восток – М. К.), а ведь до этого мнение арабов во многом зависело от CNN и BBC,... При этом большинство экспертов пришли к выводу, что «горячие новости» телекомпании «Аль-Джазира» стали в 2000-х годах частью политики»[279].

В настоящее время освещение «Аль-Джазирой» событий в Сирии способствует разжиганию агрессии против этого арабского государства и коренным образом противоречит внешнеполитическим интересам нашей страны.

---

[278] Там же.

[279] Косов Ю. В., Патаман С. Канал влияния. Почему «Аль-Джазира» побеждает конкурентов в информационной борьбе // Санкт-Петербургские ведомости. 2011. 20 мая. С. 4.

Второе направление распространения рассматриваемых угроз обусловлено деятельностью частных PR-агентств, выполняющих задания по ведению подрывных операций против других стран в информационном пространстве. Такой вид враждебной информационной деятельности зародился в Соединенных Штатах для поддержки агрессивной внешней политики этой страны, прежде всего, для вмешательства во внутренние дела других государств, включая и военные вторжения.

Информационные атаки, организуемые, по заданию американского правительства, частными PR-агентствами, могут проводиться и для оказания давления на определенное государство с целью изменения внутренней политической ситуации в нем и его внешней политики.

«В США существует практика, – отмечает Т. Б. Аничкина, – передачи части полномочий спецслужб в сфере ведения «информационных войн» нанятым по контракту частным PR-агентствам. Такие «независимые подрядчики» все чаще берут на себя функции, долгое время бывшие исключительной прерогативой специально обученных служащих ЦРУ.

В последние годы подобные агентства начали заменять региональных начальников, которые управляют секретными операциями во всем мире; оперативных дежурных в круглосуточном кризисном центре ЦРУ; аналитиков, через которых проходят разведданные; и даже контрразведчиков, отвечающих за встречи агентов и их осведомителей»[280].

Данные методы ведения информационной войны впоследствии стали использовать и другие государства, тесно связанные с США и которым американская сторона передала свой опыт и предоставила техническую и организационно-политическую помощь. Информационную войну против России, при поддержке стран Запада, развязало бывшее руководство Грузии во время конфликта на Кавказе в августе 2008 года.

[280] Аничкина Т. Б. О некоторых приемах «информационной войны США» // США – Канада. Экономика, политика, культура. № 7. Июль 2007. С. 123–127.

В ходе этого конфликта мировые информационные агентства и глобальные телевизионные сети, находящиеся под контролем, демонизировали образ России, выдавая ее за агрессора и захватчика. Материалы из зоны конфликта прозападными СМИ подавались крайне тенденциозно, осуществлялись прямые информационные подлоги и фальсификации. Таким образом, освещение конфликта представляло собой спланированную кампанию, которой руководили работающие на грузинское правительство и его западных покровителей PR-агентства.

«Западные PR-конторы, отрабатывая свою зарплату, нагло перевирали события, происходящие в Южной Осетии, подсовывая липовых очевидцев, искажая факты, опровергая или подвергая сомнению истинную информацию. В самой Грузии вырубили российские и пророссийские источники массовой информации, обвинив Россию в проведении информационной войны против Грузии. Запад поставил мировой рекорд по вранью, подлогам и переворачиванию событий с ног на голову. Масштабы были поистине гигантскими»[281].

Третье направление возникновения угроз информационной безопасности нашей страны, связанное с международной составляющей, имеет непосредственное отношение к сетевым коммуникациям. В наши дни эти коммуникации составляют новую дополнительную структуру современного общества. Широкое распространение информационно-коммуникационных технологий изменило представления о пространстве, сблизило отдельных людей, а также страны и регионы.

Структура сетей, контуры сетевых потоков, процедуры вхождения и выхода из сетевых структур, которые определяют специалисты по информационно-коммуникационным технологиям, оказывают влияние на основные тенденции современного глобального и регионального развития. В то же время, сетевые коммуникации являются во многих случаях трансграничными и выступают в качестве каналов зарубежного влияния на многие страны, включая Россию.

---

[281] Информационная война против России. URL: http://schta.ru/index.php/history-rus/85-informacionnaja-vojna-protiv-rossii. (дата обращения: 21.11.2013)

В данной связи Т. В. Владимирова пишет: «Отсутствие компетенций в сфере определения и прогнозирования сетевых коммуникативных процессов ведет к обострению проблемы информационной безопасности. Виртуальная социальная реальность, структурируемая сетевыми коммуникациями, не знает ограничений, сформированных традиционными социальными нормами; это мир, лишенный социального порядка – в традиционном его понимании.

С другой стороны, это ускользающий мир, где интенсивность коммуникаций всякий раз возрастает, отдаляя возможности его адекватного осмысления. Названные два момента в особенностях социальной виртуальной реальности сетевого коммуникативного пространства уже закладывают проблематику безопасности общества и призывают к ответственности человеческий разум»[282].

Непосредственно связаны с внешнеполитическими и международными аспектами деятельности нашего государства «угрозы информационному обеспечению государственной политики Российской Федерации». Проведение нашей страной собственного независимого политического курса в международном сообществе является важным неотъемлемым правом российского государства и его привилегией в мировой политике.

Не многие государства на нашей планете обладают возможностями для проведения самостоятельной внешней политики. Однако, в современных условиях, когда научно-технический прогресс оказывает все большее влияние на развитие международных отношений, современные технологии используются в международной политической борьбе, и в настоящее время среди них особенно выделяются, по своей роли и значимости для мирового политического развития, информационно-коммуникационные технологии.

Информационная поддержка внешней политики, отражение информационных компаний и атак, направленных на противодействие усилиям нашей страны в международных отношениях, является важной практической

[282] Владимирова Т. В. Сетевые коммуникации как источник информационных угроз //Социологические исследования. № 5. Май 2011. С. 128.

задачей как российской дипломатии, так и других государственных структур в плане обеспечения информационной и, в целом, национальной безопасности страны.

Все большее значение в современных условиях приобретает проблема формирования позитивного образа нашей страны в международном сообществе. Существенное влияние на решение этого вопроса оказывают процессы, протекающие в глобальном информационно пространстве.

В данной связи к интересным выводам пришла группа исследователей из Санкт-Петербургского университета во главе с К. К. Худолеем. Авторы отмечают: «Важной особенностью информационного поля является некоторое несоответствие спроса на информацию о России среди пользователей тому предложению, которое исходит от традиционных СМИ. Соответственно, существуют хорошие возможности использования этого факта в продвижении информации о России в рамках внешнего измерения российской информационной политики.

В целом, данные показывают, что практически все структуры, предназначенные для продвижения «более объективного» имиджа России (канал «Russia Today», Радиостанция «Голос России», информационное агентство «РИА Новости», фонд «Русский мир», журнал «Russia Profile», дискуссионный клуб «Валдай», сеть центров российской культуры и науки Российского сотрудничества, совместные проекты «Российской газеты» с ведущими зарубежными изданиями), максимально используют свой потенциал, ограниченный лишь существующим в России подходом к продвижению внешнего образа России»[283].

Международный фактор играет существенную роль в создании угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи. В настоящее время обеспечение потребностей внутреннего рынка России продукцией информационных

[283] Худолей К. К., Болотов Д. А., Трещенков Е. Ю., Седов А. М., Максимова Д. И. Россия в информационном поле зарубежных СМИ и в Интернете в 2011 г.: модели восприятия и механизмы формирования. СПб, 2011. С. 49.

технологий осуществляется во многом за счет зарубежных поставок или путем конечной сборки в нашей стране из комплектующих, поставляемых из-за границы.

Информационно-телекоммуникационная отрасль России в значительной степени зависит от внешних инвестиций, высок уровень зарубежного присутствия в акционерном капитале крупнейших телекоммуникационных компаний. Подобная ситуация создает потенциальную угрозу для потери стратегического управления информационно-телекоммуникационной отраслью в нашей стране.

В данной связи эксперты приходят к следующему выводу: «Недостаточное внимание государства к укреплению и развитию отраслей, влияющих на информационный прогресс, будет фактором постоянного нарастания угроз национальной безопасности, а в итоге может стать причиной разрушения суверенитета.

Единственный выход из этой ситуации – развитие национальной инфосферы на основе использования средств вычислительной техники и телекоммуникаций, операционных систем и прикладного программного обеспечения отечественной разработки. В первую очередь информационные системы на отечественном оборудовании должны начать вытеснять зарубежные в государственных учреждениях, силовых ведомствах, в министерстве обороны, на всех объектах критической инфраструктуры»[284].

Широкое использование зарубежных информационных технологий, заимствованных у высокоразвитых индустриальных стран без соответствующей их адаптации с целью обеспечения национальной безопасности российского государства, а также отсутствие в достаточной мере отечественных разработок в информационно-коммуникационной отрасли народного хозяйства ведет к созданию окон уязвимости. Вероятный противник, используя эти «окна», окажется в состоянии наносить реальный ущерб как военной, так и промышленной структуре государства.

---

[284] О глобализации, информатизации и национальной безопасности России. Аналитический обзор / Под ред. С. А. Таразевича. СПб: Телерос, 2010. С. 83.

Подобные случаи уже зафиксированы специалистами в области информационной безопасности, хотя, по понятным причинам, выявить, а тем более придать гласности подобные инциденты в значительном объеме не представляется возможным, так как они, как правило, осуществляются в форме тайных специальных операций. Однако, хорошо осведомленные эксперты, в некоторых случаях, приводят данные о подобных операциях.

В данной связи представляет интерес статья У. Кларка, бывшего Верховного главнокомандующего Объединенными вооруженными силами НАТО в Европе (1997–2000 гг.), и П. Левина – основателя и руководителя компании по кибербезопасности «DAFCA», посвященная вопросам усовершенствования системы электронной защиты США.

Авторы приводят следующие примеры: «В 1982 году взрыв мощностью 3 килотонны разорвал трубопровод природного газа в Сибири; вспышка была настолько сильной, что ее можно было увидеть из космоса. Два десятилетия спустя обозреватель «The New York Times» Уильям Сэфайер описал это событие как кибероперацию, спланированную и осуществленную ЦРУ. Согласно источникам, которыми пользовался обозреватель, США тщательно подготовили операцию по внедрению бракованных чипов и программ с дефектами в цепочку поставок СССР, с тем, чтобы на месте они дали сбой»[285].

Наряду с примером из времен «холодной войны», американские аналитики приводят события произошедшее уже в XXI веке, и вызвавшее много вопросов у специалистов по обеспечению национальной безопасности во всем мире.

У. Кларк и П. Левин пишут далее: «Позже известный технический журнал «IEEE Spectrum», пользуясь неподтвержденными данными, сообщал об израильском авианалете и бомбардировке предположительно ядерного объекта в Сирии в сентябре 2007 года. Успех операции объяснялся тем, что на сирийской радиолокационной станции (РЛС) была установлена система аварийного

[285] Кларк П., Левин П. Обеспечение безопасности информационной магистрали. Как усовершенствовать системы электронной защиты США // Россия в глобальной политике. 2010. Март-апрель. Т. 8. № 2. С. 178.

отключения («kill switch»), контролируемая с помощью дистанционного управления, которая и отключила РЛС кругового обзора»[286].

Очевидно, тайная война против Сирии началась не сегодня, и первые залпы в ней были сделаны, вероятно, с помощью кибероружия.

Российская Федерация уделяет огромное внимание вопросам обеспечения информационной безопасности в современном глобальном мире. В сфере международных отношений особое внимание обращается на международно-правовое обеспечение глобальной и национальной информационной безопасности.

В конце 1990-х – начале 2000-х годов. наша страна инициировала в международном сообществе начало работы по нормативному закреплению межгосударственного сотрудничества по укреплению международной информационной безопасности.

Во-первых, значительную роль в этой работе сыграли двухсторонние совместные межведомственные консультации с экспертами из США, Китая, Индии и других стран.

Во-вторых, активное сотрудничество по проблемам международно-правовых аспектов информационной безопасности осуществлялось в рамках Организации Объединенных Наций, а также других авторитетных международных институтов: таких, как «Группа восьми», Шанхайская организация сотрудничества, Международный комитет Красного Креста.

В-третьих, проблемы обеспечения информационной безопасности в 2000-е годы начали рассматриваться в контексте построения информационного общества на национальном, региональном и глобальном уровнях. Были выдвинуты подходы к решению этих проблем, согласно которым, они оказались тесным образом связаны с формированием глобального единого информационного пространства и информационной инфраструктуры.

Закреплены эти подходы были в ходе двух Встреч на высшем уровне по вопросам информационного общества в Женеве (2003 г.) и в Тунисе (2005 г.),

[286] Там же.

Россия весьма активно поддерживала эти инициативы. В ходе этих встреч были закреплены две декларации и план действий. В результате чего, у человечества появился возможный ориентир в области развития в этой сфере[287].

Наряду с дипломатической деятельностью в сфере международной безопасности на глобальном уровне, Российская Федерация проводит большую работу по развитию сотрудничества с ближайшими соседями: в частности, с теми из них, уровень доверия к которым максимально высок.

В данной связи следует упомянуть принятую в 2006 году «Концепцию формирования информационного пространства Содружества Независимых Государств». В этом документе, в целом, недостаточно развернута, но четко прописана необходимость коллективного обеспечения информационной безопасности[288].

Сам документ послужил лишь поводом к интенсификации работы в этом направлении на многостороннем уровне и подготовил переход к следующему этапу.

В сентябре 2011 года в Екатеринбурге, на второй международной встрече высоких представителей, курирующих вопросы безопасности, был представлен подготовленный российской стороной проект концепции «Конвенции ООН об обеспечении международной информационной безопасности».

Этот документ является результатом многолетней работы экспертов Совета Безопасности и Министерства иностранных дел России, а также Института проблем информационной безопасности Московского государственного университета.

В качестве основных угроз в информационном пространстве, приводящих к нарушению международного мира и безопасности, в концепции конвенции рассматриваются следующие:

---

[287] Подробнее см.: Современная мировая политика: Прикладной анализ / Отв. ред. А. Д .Богатуров. М.: Аспект Пресс, 2010. С. 477–490..

[288] Косов Ю. В., Торопыгин А. В. Проблема безопасности государств – членов Евразийского экономического сообщества // Управленческое консультирование. Актуальные проблемы государственного и муниципального управления. 2005. № 2. С. 100–107.

1) использование информационных технологий и средств для осуществления враждебных действий и актов агрессии;

2) целенаправленное деструктивное воздействие в информационном пространстве на критически важные структуры другого государства;

3) неправомерное использование информационных ресурсов другого государства без согласования с государством, в информационном пространстве которого располагаются эти ресурсы;

4) действия в информационном пространстве с целью подрыва политической, экономической и социальной систем другого государства, психологическая обработка населения, дестабилизирующая общество;

5) использование международного информационного пространства государственными и негосударственными структурами, организациями, группами и отдельными лицами в террористических, экстремистских и в иных преступных целях; и другие[289].

В первой декаде июня 2012 года в Санкт-Петербурге состоялась уже Третья Международная встреча высоких представителей, курирующих вопросы безопасности. В ней приняли участие делегации от 59 стран, представлявшие советы безопасности, аппараты президентов и глав правительств, министерств и ведомств, отвечающих за безопасность своих стран, а также от Управления по наркотикам и преступности ООН и Международной морской организации.

На этой встрече было продолжено начатое в Екатеринбурге обсуждение предложенного российской стороной вышеуказанного проекта конвенции ООН «Об обеспечении международной информационной безопасности».[290]

По мнению российских экспертов, представленный нашей страной проект конвенции ООН во многом «является противовесом известной Будапештской конвенции (Конвенции Совета Европы по киберпреступности), которую

---

[289] См.: Конвенция об обеспечении международной информационной безопасности (концепция) // http://www.scrf.gov.ru/documents/6/112.html. (дата обращения: 18.01.2014)

[290] Концепция Конвенции об обеспечении международной информационной безопасности [Электронный ресурс] / Разработана ИПИБ МГУ; представлена Россией 21-22 сентября 2011 года в Екатеринбурге на Второй Международной встрече высоких представителей, курирующих вопросы безопасности. – Режим доступа: http://www.aciso.ru/news/3255. (дата обращения: 18.10.2012)

Вашингтон пытается навязать как документ «глобального» характера в вопросах кибербезопасности».

В данной связи А. Новацкий пишет: «Россию категорически не устраивает в Будапештской конвенции как минимум 32-я статья о «трансграничном доступе», позволяющая спецслужбам одних стран проникать в компьютерные сети других стран и проводить там операции без ведома национальных властей. Долгое время российская сторона пыталась убедить европейцев убрать это нарушающее государственный суверенитет положение или отредактировать его, но страны-подписанты, поддерживаемые США, категорически отказываются вносить какие-либо изменения в документ. Логичным шагом для России в этом случае стал отказ от подписания Будапештской конвенции»[291].

Российская позиция состоит в том, чтобы рассматривать возможное противоправное использование информационных технологий во всех сферах, где они применяются.

Таким образом, под запрет или ограничение в конвенции подпадают, например, информационно-психологические операции и другие подобные виды враждебного воздействия. Американская сторона настаивает на том, чтобы ограничиться вопросами предотвращения киберугроз.

4.2. Информационная безопасность в контексте геополитики России

В современных условиях при исследовании вопросов обеспечения информационной безопасности Российской Федерации, особое внимание обращается на изучение роли и места геополитических факторов мирового развития. Эти факторы, прежде всего, связаны с защитой национальных интересов нашей страны в условиях становления новой геополитической модели мира.

---

[291] Новацкий А. Борьба вокруг проекта Конвенции ООН о международной информационной безопасности // Фонд стратегической культуры. Электронное издание. URL: http://www.fondsk.ru/pview/2012/07/14/borba-vokrug-proekta-konvencii-oon-o-mezhdunarodnoj-informacionnoj-bezopasnosti-15499.html. (дата обращения: 21.11.2013)

Так, в «Концепции внешней политики Российской Федерации» (редакция 2013 года) отмечается: «Главной, знаковой чертой современного этапа международного развития являются глубинные сдвиги в геополитическом ландшафте, мощным катализатором которых стал глобальный финансово-экономический кризис.

Международные отношения переживают переходный период, существо которого заключается в формировании полицентричной международной системы. Этот процесс проходит непросто, сопровождается повышением турбулентности экономического и политического развития на глобальном и региональном уровнях. Международные отношения продолжают усложняться, их развитие становится все более труднопредсказуемым»[292].

Указанный процесс происходит параллельно с широкой информатизацией мирового сообщества: когда новые информационные технологии оказывают все большее влияние на международные отношения. В связи с этим информационный фактор мирового развития все чаще включается в систему факторов, имеющих геополитическую природу.

В данной связи в рассматриваемом документе подчеркивается: «На передний план выдвигаются, наряду с военной мощью, такие важные факторы влияния государств на международную политику, как экономические, правовые, научно-технические, экологические, демографические и информационные»[293].

Таким образом, традиционные геополитические факторы как военная мощь государства, его демографический потенциал, экологическое измерение сочетаются с информационным фактором в качестве важных инструментов оказания влияния на международную политику.

Информационный фактор, при определении внешнеполитического потенциала государства в современных условиях, следует рассматривать в одном

---

[292] Концепция внешней политики Российской Федерации. Утверждена Президентом Российской Федерации В. В. Путиным 12 февраля 2013 г. URL: http://www.ln.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/ c32577ca0017434944257b160051bf7f. (дата обращения: 18.10.2012)

[293] Там же.

ряду не только с геополитическими, но и с экономическими, научно-техническими и правовыми характеристиками той или иной страны.

Данный подход позволяет более полно учитывать пространственные характеристики России, ведущих мировых держав и сопредельных стран при разработке и реализации политики обеспечения национальной безопасности нашего государства. В то же время, в процессе обеспечения безопасности страны, сохранения и укрепления ее суверенитета и территориальной целостности, прочных и авторитетных позиций в мировом сообществе в наше время постоянно возрастает роль информационного пространства в данном процессе.

В данной связи интересно привести мнение секретаря Совета Безопасности Российской Федерации Н. П. Патрушева: «По данным ФСБ России, только на сайты президента, Госдумы, Совета Федерации ежедневно осуществляется до 10 тысяч атак. Главной целью этих акций является нарушение работоспособности соответствующих информационных систем. Менее известны, но от этого не менее опасны компьютерные атаки, направленные на нарушение функционирования крупных кредитно-банковских структур, объектов экономической и социальной сферы, систем жизнеобеспечения»[294].

Сложившееся положение дел требует детального изучения, поскольку существенным образом влияет на изменение геополитической ситуации при обеспечении национальной безопасности нашей страны.

Анализ особенностей обеспечения национальной безопасности в информационном пространстве, с позиций геополитики, обусловлен следующими причинами.

Во-первых, анализ подобного рода вносит важный вклад в формирование научного обеспечения комплексного подхода к разработке и реализации концепции национальной безопасности России и к ее важной составляющей – системе мер по обеспечению информационной безопасности.

Во-вторых, изучение геополитических факторов в тесной взаимосвязи с информационным фактором мирового развития позволяет рассматривать

[294] Патрушев Н. П. ФСБ раскинет сеть // Российская газета. 2013. 20 февраля. № 36(6012). С. 17.

международные процессы с учетом их стремительного ускорения в настоящее время и усиления новых тенденций в трансформации глобального сообщества.

Такой подход может быть полезен для разработки адекватной политическим реалиям современного мира политики информационной безопасности. Эта политика должна стать важной составляющей системы мер по обеспечению национальной безопасности Российской Федерации, включая и противодействие угрозам в информационном пространстве.

На формирование такой политики направлен Указ Президента Российской Федерации «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», подписанный 15 января 2013 года.

Как сказано в документе, «функциональные возможности системы должны не только ликвидировать последствия кибератак на государственные информационные ресурсы, но и обеспечить их раннее обнаружение, а в перспективе – и предупреждение таких инцидентов»[295].

В-третьих, геополитический подход имеет принципиальное значение для осмысления участия России в процессах глобализации, которые непосредственно связаны с информационными процессами как на мировом, так и на региональном уровнях. Большое влияние глобализация оказывает и на состояние информационной безопасности во всемирном масштабе.

Так, современные достижения научно-технического прогресса сделали возможным создание глобальных информационных структур: в частности, глобальной системы Интернет, глобальных медийных сетей и телекомпаний. Подобного рода системы способны оказывать существенное влияние на международно-политическую ситуацию в мире, являясь важным инструментом информационного сопровождения внешнеполитической деятельности наиболее развитых государств.

---

[295] Цит. по: Кибербезопасность РФ: щит и меч для защиты информации // URL: http://www.rusnevod.com/cgi-bin/rnev/start.cgi?prn1=info2&grp=0208. (дата обращения: 12.02.2014)

Глобализация порождает и новые угрозы и опасности, распространяющиеся через глобальное информационное пространство. «На первый план в современной международной политике выходят имеющие трансграничную природу новые вызовы и угрозы; стремительно возрастают их уровни, диверсифицируются их характер и география. Прежде всего, это опасность распространения оружия массового уничтожения и средств его доставки, международный терроризм…, угрозы информационной и продовольственной безопасности»[296].

В-четвертых, новые информационные технологии в международных отношениях создают благоприятные условия для расширения и демократизации сферы дипломатической деятельности. Они играют важную роль в развитии публичной (или народной) дипломатии, которую в последнее время стали обозначать термином, взятым из арсенала информационных технологий (IT) – «Дипломатия 2.0».

Все шире применяются в международной политике, наряду с такой альтернативной дипломатией, отличной от традиционных дипломатических подходов, базирующихся на обычаях, сложившихся в предыдущие века, и другие подходы. Они связаны с оказанием влияния и воздействия на мировые и региональные процессы с помощью использования ресурсов в культурной, гуманитарной и других сферах, не связанных с применением силы или политического давления. Такой подход получил название «мягкая сила».

В «Концепции внешней политики Российской Федерации» (редакция 2013 года) написано: «Неотъемлемой составляющей современной международной политики становится «мягкая сила» – комплексный инструментарий решения внешнеполитических задач с опорой на возможности гражданского общества, информационно-коммуникационные, гуманитарные и другие альтернативные классической дипломатии методы и технологии»[297].

---

[296] Концепция внешней политики Российской Федерации. Утверждена Президентом Российской Федерации В. В. Путиным 12 февраля 2013 г. URL: http://www.ln.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/c32577ca0017434944257b160051bf7f. (дата обращения: 14.09.2013)

[297] Там же.

Во втором десятилетии XXI века информационно-коммуникационные технологии стали все шире внедряться в процессе применения «мягкой силы», а в некоторых случаях эти технологии стали занимать доминирующее положение при реализации данной формы внешнеполитической деятельности. В данной связи появился также термин «Мягкая сила 2.0». Возникновение такого феномена явилось отражением сближения процессов информационного и политического развития международного сообщества в условиях глобализации.

А. И. Смирнов и И. Н. Кохтюлина, рассматривая данный феномен, пишут: «Начало второго десятилетия XXI в. ознаменовалось качественно новым этапом информационной революции – политизацией. Ее феномен стал не только локомотивом глобализации, но и нервом, поскольку, наряду с несомненным позитивом, породил ряд принципиально новых геополитических вызовов и угроз»[298].

Остановимся более подробно на указанных вызовах и угрозах, чтобы выяснить, чем вызван их геополитический характер.

Распространение новых информационных технологий в последние годы привело к широкой компьютеризации международного сообщества, которая охватила не только развитые, но проникла и в развивающиеся регионы. Распространение скоростного доступа к сети Интернет сделало общение в этой системе чрезвычайно динамичным и информационно емким. На сегодняшний день, виртуальное информационное пространство Интернета, по своему влиянию на сознание и по роли в формировании общественного мнения, обошло средства массовой информации (СМИ). Таким образом, использование интернет-ресурсов оказывает реальное влияние на основные сферы жизнедеятельности обществ отдельных стран, на региональные сообщества и на человечество в целом.

В 2012 году, впервые в истории, был определен Веб-индекс (Web-Index), учитывающий количество и качество использования Интернет-ресурсов в 61 стране (в дальнейшем планируется расширить этот список до 100 стран). «Место

[298] Смирнов А. И., Кохтюлина И. Н. Глобальная безопасность и «Мягкая сила 2.0»: вызовы и возможности для России. М.: ВНИИгеосистем, 2012. С. 58.

той или иной страны в рейтинге определяется, исходя из семи факторов, среди которых: степень влияния Сети на политику, экономику и общество в этой стране, а также степень развитости веб-инфраструктуры»[299].

Как видно, эксперты уже при составлении первого Веб-индекса поставили влияние Всемирной паутины на политику на первое место. По мнению многих аналитиков, велико влияние Интернета на важнейшие политические процессы в современном мире: такие, как дестабилизация региона Ближнего Востока, протестные движения в Европейском Союзе в условиях нынешнего кризиса, движение антиглобалистов, выборы президентов США, России и так далее.

Приведенные факты показывают, что новые информационные технологии превратились в весьма значимый фактор, который способствуют осуществлению существенных геополитических изменений в современных международных отношениях, оказывает немалое влияние при выборах государственного руководства в ведущих странах, которое формирует геополитические стратегии поведения ведущих глобальных и региональных игроков на мировой арене.

Некоторые исследователи обращают внимание на роль виртуальных коалиций как субъектов геополитических процессов, имеющих характер конкурентного соперничества.

А. И. Смирнов и И. Н. Кохтюлина приходят к следующему выводу: «Виртуальные коалиции – это субъекты геополитической конкуренции, в которые могут входить государства, региональные структуры, транснациональные корпорации, глобальные социальные сети, медиа-холдинги и так далее. Информационно-коммуникационные технологии позволяют виртуальной коалиции быстро приспосабливаться к изменениям внутренней и внешней геополитической ситуации, маневрировать силами и средствами, быстро восстанавливать свой потенциал после неудач и гибко подбирать для каждого из субъектов адекватные формы реагирования»[300].

---

[299] Россия заняла 31-е место в интернет-рейтинге. 06.09.2012 // URL: http://www.sostav.ru/news/2012/09/06/rossiya_31_mesti_internet_reyting. (дата обращения: 06.09.2012)

[300] Смирнов А. И., Кохтюлина И. Н. Указ. соч. С. 72.

Ведущую роль в этих виртуальных коалициях играют виртуальные социальные сети и медиакорпорации, для которых характерны следующие отличительные черты:

− обладание значительным информационно-технологическим потенциалом;

− контроль со стороны различных ведущих финансово-промышленных групп;

− тесная связь с национальными и международными политическими элитами;

− наличие возможностей для распространения информации в неполном (или искаженном) виде с целью манипулирования общественным мнением;

− расположение сетевых ресурсов на территории нескольких, а иногда и весьма значительного числа государств, что способствуют возникновению ситуаций, когда вмешательство одного правительства в деятельности сети или корпорации с целью продвижения своих геополитических интересов может нанести реальный вред другому государству (или группе стран).

Крупнейшей социальной сетью в мире является «Facebook», которая была основана в 2004 году. Уже на 4 октября 2012 года, аудитория «Facebook» составила свыше 1 млрд. пользователей. Суточная активная аудитория в марте составила 526 млн. человек – столько фиксируется следящей сетью «Facebook» ежедневно. Около 500 млн. человек в месяц используют мобильное приложение «Facebook».

Каждый день в социальной сети пользователи оставляют 3,2 млрд. «лайков» и комментариев и публикуют 300 млн. фотографий. На сайте зафиксированы 125 млн. «дружеских связей» (на 31 декабря 2011 года было 100 млн.). Количество просмотров страниц сайта в октябре 2011 года составило более 1 трлн.[301].

Приведенные выше угрозы национальной безопасности России, возникшие в результате внедрения в международные процессы новых информационных технологий и имеющие геополитический характер, требуют, для их изучения и

[301] Facebook // URL: http://ru.wikipedia.org/wiki/Facebook.

осмысления, проведения соответствующего анализа с позиций современной геополитической теории. Такой анализ базируется на представлении о геополитике системе междисциплинарных знаний о внешнеполитическом потенциале государства, основу которого составляют естественно-природные и социальные ресурсы, в которых постоянно возрастает их информационная составляющая.

Использование (или обладание) данным потенциалом позволяет современному государству защищать национальные интересы и достигать внешнеполитические цели на мировой арене. При этом географическая среда и другие природные характеристики государств рассматриваются в тесной взаимосвязи с важнейшими внешнеполитическими и международными процессами, в том числе и в глобальном и региональном информационных пространствах.

Эти процессы определяют статус государств в международном сообществе и мировом информационном пространстве, а также их внешнеполитические возможности, включая и внешнеполитический информационный потенциал. К данным процессам, прежде всего, автор относит следующие:

− достижение информационного превосходства в процессе геополитической конкуренции на информационном пространстве;

− проведение информационной политики в контексте геополитических процессов;

− обеспечение информационной безопасности в рамках геополитических процессов.

Рассмотрим данные процессы более подробно с учетом реалий современного глобального мира.

1) Информационное превосходство некоторые исследователи справедливо рассматривают как форму реализации геополитической конкуренции в информационном пространстве[302].

[302] См., например. Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны. М.: Горячая линия – Телеком, 2012. С. 97.

Геополитическая конкуренция отражает претензии, соперничество или борьбу двух (или более) держав за контроль над определенным геополитическим пространством (или линией).

Наибольшие по своим размерам и самые значимые по своей роли в международных процессах пространства называются геостратегическими регионами. Они, в свою очередь, подразделяются на геополитические регионы и субрегионы, которые, как правило, становятся объектами геополитической конкуренции.

Большое значение в геополитической конкуренции имеет соперничество за контроль над геостратегическими линиями. «Важную роль в формировании геополитического пространства играют так называемые геостратегические линии. Под ними понимают оси, вокруг которых идет процесс геополитического структурирования и организации пространства в определенном регионе.

В качестве таких линий обычно выступают: сухопутные и морские коммуникации (железные и шоссейные дороги, морские и океанские пути движения судов и тому подобное); направления распространения культур, религий, идеологий, линии сотрудничества или соперничества между государствами»[303].

В современных условиях конкуренция между государствами переместилась в информационное пространство и ведется также за образующие каркас этого пространства информационно-коммуникационные каналы, некоторые из которых являются трансконтинентальными.

Таким образом, информационный фактор в наши дни начинает играть все большую роль в геополитической конкуренции. Государство, обладающее значительным информационным потенциалом и способное эффективно его применять для достижения внешнеполитических целей и защиты национальных интересов в глобальном или региональном масштабах, существенно усиливает

[303] Косов Ю. В. Мировая политика и международные отношения // Политология: Учебник для вузов / Под ред. М. А. Василика. Рекомендовано Министерством общего и профессионального образования Российской Федерации в качестве учебного пособия для студентов высших учебных заведений. М.: Гардарики, 2008. С. 71.

свою мощь: то есть способность воздействовать в выгодном для себя смысле на международные процессы.

Как известно, «важным элементом геополитического анализа является сила (или мощь) государства. Категория «сила» отражает чрезвычайно сложное и многофакторное геополитическое явление. С одной стороны, сила государства – это способность одной державы достигать своих целей во внешней политике путем оказания существенного (или определяющего) воздействия на политику других стран.

С другой стороны, сила связана с возможностями государства отстаивать свои интересы, самостоятельно решать жизненно важные задачи своего политического и экономического развития»[304].

На основании вышеизложенного можно сделать вывод, что геополитический анализ информационного пространства современных международных отношений и влияния новых информационных технологий на изменение геополитических характеристик международных процессов нашего времени представляет собой актуальную исследовательскую задачу для политической науки, имеющую как теоретическое, так и практическое значение.

На формирование геополитического подхода к изучению информационного пространства в контексте глобальных и региональных международных процессов определенное влияние оказал уже накопленный в политологических исследованиях опыт геополитического анализа воздушно-космического пространства.

В данной связи А. В Манойло, А. И Петренко и Д. Б. Фролов пишут: «Эволюция взглядов на включение информационно-психологического пространства в сферу геополитической конкуренции и перенесения (проецирования) на эту сферу законов геополитики была подготовлена распространением геополитической конкуренции на воздушную среду – особенно с созданием бомбардировочной авиации, когда стало ясно, что стратегическая значимость тех или иных регионов неизбежно изменится… Еще более

[304] Там же. С. 165.

пространственно-временное содержание геополитической конкуренции изменилось с выходом в воздушно-космическое пространство»[305].

Автор данного диссертационного исследования в своих работах уже достаточно подробно рассматривал превращение воздушно-космического пространства в одну из основных арен современных геополитических процессов в результате интенсивного развития человеческой деятельности в этой сфере.

В начале прошлого столетия были созданы летательные аппараты, способные перемещаться в воздушной среде. Вскоре воздушное пространство превратилось и в сферу вооруженного противоборства. Развитие воздушных вооружений значительно опережало совершенствование средств ведения борьбы сухопутных и морских сил. Ведущая роль военно-воздушных проявилась уже в годы Второй Мировой войны, а затем и в последующих локальных войнах и конфликтах второй половины XX века.[306].

Геополитический анализ информационного пространства показывает, что особое значение при развертывании конкуренции в нем играют информационные ресурсы. Их наличие меняет характер геополитической конкуренции в информационном пространстве как составляющей части геополитического региона.

Данная конкуренция в качестве принципиально важного направления включает борьбу за господство в информационном пространстве. Достижение такого господства зависит от обладания информационными ресурсами, которые по своим качественным и количественным показателям значительно превосходят подобные ресурсы конкурирующей стороны.

«Информационный ресурс является совершенно особой составляющей в совокупности ресурсов развития. Его объекты и объединяющая их

---

[305] Манойло А. В., Петренко А. И., Фролов Д. Б. Указ. соч. С. 98.

[306] См.: Кучерявый М. М. Система обеспечения национальной безопасности Российской Федерации в воздушно-космическом пространстве: политологический анализ. Диссертация на соискание ученой степени кандидата политических наук. СПб, 2009. 219 с.; его же, Космическое измерение военной безопасности Российской Федерации: геополитический анализ // Власть. 2009. № 1. С. 7–12; его же, Геополитический анализ современных международных процессов и обеспечение национальной безопасности России в воздушно-космическом пространстве // Известия РГПУ им. А.И. Герцена. 2009. № 12 (89). С. 9–101; его же, Геополитические противоречия между Россией и Западом в воздушно-космической сфере // Управленческое консультирование. 2009. № 1. С. 68–75.

информационная инфраструктура имеют особые пространственно-временные характеристики, не ограничиваемые пределами национальной территории. Кроме того, сама информация как базовый и наиболее универсальный элемент этого ресурса обладает уникальными свойствами делимости и воспроизводимости, что заметно сказывается на общей оценке потенциала того или иного геополитического субъекта…»[307].

Процесс информатизации современного международного сообщества протекает в наши дни одновременно с процессом изменения и усложнения геополитической структуры мира. Взаимовлияние двух этих процессов оказывает существенное влияние на политическое развитие современных международных отношений. Расширяется число акторов международных отношений, в том числе и за счет дифференциации внутри геополитической структуры.

Увеличивается и число связей между участниками международной жизни. Такому увеличению в значительной степени способствовало формирование глобального, регионального и национальных информационных пространств.

В этих пространствах возникает взаимодействие, приводящее, при определенных условиях, к геополитической конкуренции между различными державами и другими субъектами международных отношений. Данный феномен обуславливает увеличение роли информационных ресурсов в современных геополитических процессах. Уровень развития этих ресурсов зависит от интеллектуального и научно-технического потенциалов соответствующего государства.

Большое значение имеет также степень подготовленности политической и военной элит государства к руководству страной, находящейся в условиях информационного общества. От действий этих элит зависит эффективность применения информационных ресурсов в процессе геополитической конкуренции или противоборства на мировой арене либо в мирное, либо в военное время.

Возрастание значимости информационных ресурсов в международных процессах ведет, в известной мере, к уменьшению роли материальных,

[307] Манойло А. В., Петренко А. И., Фролов Д. Б. Указ. соч. С. 98.

энергетических и пространственных (в географическом смысле) ресурсов при определении геополитического потенциала современного государства. При этом происходит определенное увеличение геополитической значимости информационного и космического пространства, что уже отмечалось ранее.

Прежде всего, такие изменения касаются военной сферы. Например, В. И. Мизин отмечает: «Сегодня практически похоронена идея «бесконтактных» войн, идея «роботизации войн». Основные арены битв в течение века будут переноситься с наземно-воздушного пространства в два других – космическое и в Интернет. Информационно-коммникационные военные технологии или информационное оружие будут постепенно вытеснять ядерное в качестве «сверхоружия» XXI века. Если и появляются новые технологии, то они используются у развитых государств.

Но и те вооруженные силы третьего мира, которые действуют в «серых зонах», в непризнанных государствах, приспосабливаются к новым методам ведения боевых действий, к новым технологиям в вооружениях. И под технологиями здесь следует понимать не только новую электронику, новую авионику и так далее, но и средства связи, и организации вооруженной борьбы»[308].

Следует отметить, что многие эксперты считают: говорить сегодня о вытеснении ядерного оружия информационным оружием или какими-то иными инновационными средствами ведения боевых действий пока преждевременно. Ядерное сдерживание продолжает играть важную роль в обеспечении глобальной безопасности и поддержании геополитического баланса сил в мировом сообществе.

«Как известно, – пишет А. Г. Савельев, – ядерное оружие рассматривается в качестве оружия сдерживания возможной агрессии. Условно говоря, сдерживать

[308] Мизин В. И. Новые аспекты стратегии национальной безопасности // Вестник МГИМО-Университета. 2012. № 6 (27). С. 26.

агрессора можно, пугая его тем, что ты применишь ядерное оружие первым или обладаешь потенциалом для ответного удара»[309].

В то же время, существует опасность распространения ядерного оружия, когда им пытаются завладеть государства с нестабильными политическими режимами или даже террористические организации. Ведущие государства мира активно сотрудничают в обеспечении режима нераспространения ядерных вооружений.

Таким образом, можно сделать вывод, что информационное оружие не вытесняет ядерное. Для кибервооружений формируется своя ниша как в системе обороны и ведения боевых действий, так и в процессах геополитических конкуренции в современном мире, которая становится все более сложной и многомерной.

2) Цели и задачи информационной политики в контексте геополитических процессов определяются, в первую очередь, государственным строем и политической системой общества, от которых зависит организационная структура и эффективность управления обществом. В современном демократическом государстве эффективность управления обеспечивают и такие факторы, как наличие развитого гражданского общества, свобода общественной деятельности и функционирования средств массовой информации. Большое значение имеют также традиции и качество национальной дипломатии, которая обеспечивает взаимодействие с другими государствами и международными организациями.

Дипломатия, вместе с общественными организациями и средствами массовой информации, формирует имидж страны в международном сообществе, который оказывает существенное влияние на возможности внешней политики государства, включая сферу национальной и международной безопасности.

В настоящее время, в рамках «Дипломатии 2.0», активно применяются современные информационно-коммуникативные технологии для решения

---

[309] Савельев А. Г. Роль ядерного оружия в обеспечении безопасности РФ // Военно-политическая ситуация в мире и вопросы обеспечения национальной безопасности России. / Под ред. Г. Г. Тищенко и Е. С. Хотьковой. – М.: Рос. Ин-т стратегич. исслед., 2011. С. 62.

геополитических задач. Эффективность такого подхода, как показывает практика, во многом зависит от целенаправленности и качества информационной политики.

Данная политика – это сфера жизнедеятельности людей в условиях современного информационного общества, в основе которой лежат процессы сбора, обработки и распространения информации в интересах органов государственного управления и структур гражданского общества. Распространяемая в ходе реализации такой политики информация может, при определенных условиях, выходить за рамки государственной территории и национального информационного пространства.

Такой выход информации в международное информационное пространство превращает ее в важный фактор, оказывающий воздействие на геополитические процессы, а сама информационная политика представляет собой один из важных инструментов реализации внешней политики современного государства.

Рассмотрим данные явления на примере взаимодействия нашей страны с Европейским Союзом. Одним из наглядных проявлений рассматриваемого феномена в отношениях нашей страны и ЕС является информационная политика, проводимая сторонами в пространстве «общего соседства».

«Словосочетание «общее соседство» России и ЕС возникло после самого масштабного за историю ЕС расширения. 2004–2007 гг. Именно тогда соседями России на западе и ЕС на востоке стали одни и те же государства, и концепция «политики соседства» ЕС, разрабатываемая с 2003 года, наложилась на российский концепт ближнего зарубежья, существовавший с момента распада СССР и образования СНГ.

Интересно, что Россия согласилась признать в качестве «общего соседа» только Беларусь[310], Молдову и Украину. Для ЕС «общие соседи» – это еще и Азербайджан, Армения и Грузия»[311].

Очевидно, что в приведенном примере терминологические споры и разногласия по поводу стран, которые, входя в пространство «Общего соседства»,

---

[310] Об информации, информатизации и защите информации: Закон Республики Беларусь от 10.11.2008 г. № 455-З.

[311] Шишкина О. В. Внешнеполитические ресурсы: Россия и ЕС на пространстве «общего соседства». М.: Аспект Пресс, 2013. С. 16.

в завуалированной форме отражают достаточно серьезные геополитические противоречия между глобальными игроками на мировой арене – Евросоюзом и Россией.

Важную роль в продвижении и защите геополитических интересов на пространстве Восточной Европы в рамках общего соседства играют информационно-пропагандистские ресурсы как составная часть внешнеполитических ресурсов обеих взаимодействующих сторон – ЕС и РФ.

Российский исследователь О. В. Шишкина относит к основным информационно-пропагандистким ресурсам, которые используются в рассматриваемой геополитической ситуации, следующие:

– пресса, распространенность вещания, информационные центры, дома культуры;

– привлекательность на основе информации из СМИ, современная привлекательность, имидж государства;

– культурные мероприятия (дни культуры, фестивали)[312].

Таким образом, информационная политика направлена на формирование благоприятного имиджа государства, ее проводящего, на продвижение геополитических интересов, на облегчение решения внешнеполитических задач с помощью «Мягкой силы 2.0».

В данной связи можно уже говорить об информационной мощи государства, имеющей геополитическое измерение. Данная информационная мощь позволяет некоторым ведущим государствам современного мира достигать важных геополитических целей без применения силовых инструментов – вооруженных сил, политик эмбарго, блокад и бойкотов, на которые был богат предыдущий этап мирового исторического развития, известный как «холодная война».

3) Большое значение для изучения информационной безопасности имеет анализ ее геополитических аспектов. Такой подход обусловлен следующими причинами. Во-первых, геополитический анализ нацелен на оценку силового

[312] Там же. С. 25.

потенциала государства, степень его защищенности от внешних угроз и, в итоге, – определение уровня безопасности страны.

Такой анализ использует, прежде всего, пространственные характеристики государства. В наши дни следует рассматривать как важный геополитический показатель обеспечения безопасности государства конфигурацию, позиционирование и степень его защищенности в глобальном информационном пространстве.

«Глобальное информационное пространство, – как отмечает Н. Н. Ковалева, – совокупность информационных ресурсов и информационной инфраструктуры, позволяющей на основе единых принципов и по общим правилам обеспечивать безопасное информационное взаимодействие государств, организаций и граждан при их равнодоступности к открытым информационным ресурсам, а также максимально полное удовлетворение их информационных потребностей при сохранении баланса национальных и международных интересов»[313].

Как известно, на протяжении всей истории международных отношений принцип баланса сил играет важную роль в действиях государств на мировой арене. После окончания «холодной войны» исследователи международных отношений стали отмечать, что, наряду с принципом баланса сил на мировой арене, начал все чаще использоваться принцип баланса интересов.

Некоторые теоретики высказывали предположение, что баланс интересов заменит баланс сил в международных отношениях в ближайшее время. Однако, войны и вооруженные конфликты в Югославии, Ираке, Афганистане, Чечне, Грузии, Ливии, Сирии и в некоторых других странах и регионах показали, что делать вывод о прекращении применения силы в международных отношениях пока преждевременно.

Сохранение силовой политики в мире означает и актуальность в наши дни принципа баланса сил. Действия государств, на мировой арене имеющие

[313] Ковалева Н. Н. Информационное право России. М.: ИТК «Дашков и К», 2012. С. 287.

пересекающийся или сталкивающийся характер, как в глобальном, так и региональных измерениях, могут приводить к нарушению баланса сил.

В то же время, в мировой геополитике реализуется и другая тенденция – поддержание равновесия баланса сил. Если такое равновесие отвечает интересам большинства участников мировых и региональных политических процессов, то оно устанавливается и поддерживается, а субъекты, стремящиеся его нарушить, оказываются либо в изоляции, либо на периферии международных отношений. В связи с этим следует подчеркнуть, что баланс сил представляет собой динамически равновесный процесс.

Политика поддержания баланса сил является важным направлением внешней политики России и других ведущих государств современного мира.

Такая политика имеет следующие основные направления:

− обеспечение национальной безопасности государства, прежде всего ее военно-политической составляющей;

− достижение внешнеполитических целей государства, поставленных в соответствии с высшими приоритетами его национальной безопасности;

− сохранение военно-политического статус-кво в мире в целом или в конкретном геополитическом регионе;

− обеспечение условий для устойчивого и стабильного внутреннего развития государства.

Так, в «Концепции внешней политики Российской Федерации» (редакция 2013 года) в качестве одной из основных внешнеполитических целей нашего государства обозначено: «Создание благоприятных внешних условий для устойчивого и динамичного роста экономики России, ее технологической модернизации и перевода на инновационный путь развития, повышения уровня и качества жизни населения, укрепления правового государства и демократических институтов, реализации прав и свобод человека»[314].

[314] Концепция внешней политики Российской Федерации. Утверждена Президентом Российской Федерации В. В. Путиным 12 февраля 2013 г. URL: http://www.ln.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/ c32577ca0017434944257b160051bf7f. (дата обращения: 14.09.2013)

Возникновение глобального информационного пространства, несомненно, способствует более широкому распространению принципа баланса интересов в современных международных отношениях. «Концепция баланса сил – важный фактор при взаимоотношении государств на международной сцене, преследующих собственные интересы, часто не совместимые с интересами других государств. Конфликт интересов государств может привести к войне.

При этом сила становится необходимым условием для самоутверждения государства в мире. Преобладающая сила заставляет других делать то, что они не сделали бы в противном случае. Сила есть совокупность всех возможностей (военная, идеологическая, культурная и тому подобное), которые имеет политический субъект для удовлетворения своих интересов. Смысл баланса сил сводится к равновесию силовых характеристик нескольких государств»[315].

Эксперты отмечают, что баланс интересов отличается от баланса сил по ряду характеристик и параметров. Рассмотрим этим отличия, прежде всего, применительно к обеспечению информационной безопасности в контексте геополитических процессов.

Во-первых, при нахождении баланса интересов уравновешиваются не силовые потенциалы, а национальные интересы государств, а также интересы международного сообщества. Такой подход стимулируют конструктивную деятельность, и при его реализации большое значение имеет информационное обеспечение.

Во-вторых, в процессе достижения баланса интересов происходит взаимное изучение и учет сторонами интересов друг друга. Это повышает степень доверия в двух- и многосторонних отношениях, что требует увеличения информационной прозрачности и позволяет избегать больших расходов – в отличие от сохранения силового равновесия с неизбежным для этого процесса наращиванием или совершенствованием вооружений.

---

[315] Баланс интересов в управлении // URL: http://www.market-journal.com/voprosiupravleniya/79.html. (дата обращения: 11.12.2013)

В-третьих, принцип баланса интересов более подходит для информационной сферы международных отношений, чем принцип баланса сил. Это связано с сущностью информационных процессов. С их помощью государства позиционируют в международном сообществе свои интересы, формируют имидж своих стран.

Согласование интересов способствует поиску взаимовыгодных компромиссов, позволяет развивать диалог по самым сложным проблемам мировой политики. В данной связи следует признать, что в сфере международных отношений во многих случаях принцип баланса интересов оказывается более эффективным, чем принцип баланса сил.

В то же время, наряду с поиском баланса интересов или сил на мировой арене, сохраняется конкуренция между государствами, союзами государств, геополитическими регионами и международными организациями. Изменения в геополитической структуре мира ведут к смещению центров силы, изменениям в конфигурации геополитических регионов и геостратегических осей. Государства, претендующие на создание полюсов мирового развития, стремятся к доминированию и в информационной сфере.

Такого рода геополитические трансформации ведут к изменению путей информационных потоков и расположения информационных магистралей и узлов в глобальном информационном пространстве. Данные изменения воздействуют на состояние информационной безопасности всех основных субъектов международных отношений. Они влияют на массовое общественное сознание как отдельных государств, так и мирового сообщества в целом.

Подвижки в состоянии глобальной информационной безопасности вызывают сдвиги геополитических позиций основных участников конкуренции и соперничества на мировой арене. В дальнейшем подобные процессы ведут и к изменению геополитической картины в глобальном и региональном масштабах.

Приведенные выше проблемы обеспечения информационной безопасности в контексте геополитических процессов следует учитывать при формировании и реализации внешней политики нашей страны.

В «Концепции внешней политики Российской Федерации» (редакция 2013 года) сформулированы основные направления действий в этой сфере: «В рамках публичной дипломатии Россия будет добиваться объективного восприятия ее в мире, развивать собственные эффективные средства информационного влияния на общественное мнение за рубежом, обеспечивать усиление позиций российских средств массовой информации в мировом информационном пространстве, предоставляя им необходимую государственную поддержку, активно участвовать в международном сотрудничестве в информационной сфере, принимать необходимые меры по отражению информационных угроз ее суверенитету и безопасности. В этой деятельности будут широко использоваться возможности новых информационно-коммуникационных технологий»[316].

Реализация зафиксированных в документе мероприятий потребует адаптации к конкретным ситуациям в мировых и региональных политических процессах и будет занимать важное место в геополитике нашей страны.

4.3. Глобальное информационное противоборство на мировой арене

В первые десятилетия XXI века мировое развитие характеризуется высоким динамизмом, фундаментальными структурными сдвигами и противоречивостью. «Продолжают сокращаться возможности исторического Запада доминировать в мировой экономике и политике. Происходит рассредоточение мирового потенциала силы и развития, его смещение на Восток, в первую очередь в Азиатско-Тихоокеанский регион. Выход на авансцену мировой политики и экономики новых игроков на фоне стремления западных государств сохранить свои привычные позиции сопряжен с усилением глобальной конкуренции, что проявляется в нарастании нестабильности в международных отношениях»[317].

---

[316] Концепция внешней политики Российской Федерации. Утверждена Президентом Российской Федерации В. В. Путиным 12 февраля 2013 г. URL; http://www.ln.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/ c32577ca0017434944257b160051bf7f. (дата обращения: 14.09.2013)

[317] Там же.

Важным направлением глобальной конкуренции в наши дни представляет собой противоборство в информационной сфере. Такого рода изменения в мировом развитии объясняются следующими причинами.

Во-первых, одной из наиболее важных сущностных характеристик современного этапа мирового развития является становление глобального информационного общества. Основой для создания такого общества стали информационно-коммуникационные технологии. Эти технологии оказали фундаментальное влияние на образ жизни людей, сферы образования, труда, государственного управления, гражданское общество и международные отношения.

Государства, занимающие господствующие позиции в таком принципиально важном для XXI века секторе мирового развития, как становление глобального информационного общества, занимают лидирующее положение в современном миропорядке.

Во-вторых, государство, обладающее более мощным информационным потенциалом, чем его конкуренты, может эффективно отстаивать и продвигать свои национальные интересы, играть ведущую роль в мировых и региональных политических процессах. В наши дни для решения многих принципиальных проблем внешней политики, вместо широко применявшихся ранее военно-силовых средств, более эффективными оказываются информационно-пропагандистские и информационно-психологические методы.

В данной связи эксперты приходят к следующему выводу: «Доминирование в информационной сфере дает возможность успешно достигать внешне- и внутриполитические цели. Обретение информационного превосходства чаще рассматривается ведущими державами как эффективное и перспективное средство, позволяющее добиваться политических целей в ситуациях, когда применение силы невозможно или нецелесообразно. При этом информационное противоборство постепенно перемещается из военно-технологической сферы в

область формирования мировоззрения при помощи методик политического манипулирования»[318].

Как показывает опыт войн и вооруженных конфликтов начала XXI века, активно применяется и сочетание, взаимное дополнение военных и информационных методов ведения войны. Так было при вторжении США в Ирак (2003 г.), при нападении Грузии на Южную Осетию (2008 г.) и тому подобное.

В-третьих, «цифровое неравенство» все в большой степени начинает оказывать влияние на иерархию государств в мировом сообществе. Страны конкурируют за доступ к высоким информационно-коммуникационным технологиям, информационным магистралям и ресурсам. Наличие такого доступа в полном объеме создает для страны широкие возможности для продвижения своих национальных интересов в различных частях света и оказания реального влияния в нужном для себя направлении на политические и экономические процессы как регионального, так и глобального масштабов.

Ограничения на пути вхождения в глобальное информационное общество негативно влияет на возможности участия страны в современных международных отношениях или вообще отодвигает ее на периферию мирового развития.

Так, К. А. Панцерев отмечает, «что в 1990-х гг. «всеобщая информатизация» приводит к известной маргинализации, дальнейшему увеличению разрыва между имеющим доступ к современным информационным технологиям Севером и информационно бедным Югом. Мир теперь стал делиться не только на экономически развитые и экономически отсталые регионы, но еще и на информационно богатые страны, имеющие доступ к современным компьютерным технологиям, и информационно бедные государства, развитие компьютерных систем и сетей в которых находится в зачаточном состоянии»[319].

Таким образом, следует признать, что доступ к информационно-коммуникационной инфраструктуре является важной стороной конкуренции в

---

[318] Современная мировая политика: Прикладной анализ / Отв. ред. А. Д. Богатуров. – М.: Аспект Пресс, 2010. С. 221–222.

[319] Панцерев К.А. Страны Тропической Африки на пути в глобальное информационное общество: проблемы и перспективы. СПб.: СПбГУ, 2010. С. 49–50.

глобальной информационной сфере. Однако, для противоборства в указанной области имеет большое значение также способность государства не только использовать информационно-коммуникационные технологии, но быть в состоянии воспроизводить их.

Страны, в которых существует телекоммуникационная отрасль экономики как материальная основа национальной информационно-коммуникационной сферы, имеют очевидные преимущества в глобальном информационном противоборстве. В наши дни научно-техническое развитие в современной телекоммуникационной сфере обуславливается технологическими достижениями, которые связаны с широкомасштабным внедрением микропроцессорной техники и внедрением цифровых методов передачи и коммутации.

В Доктрине информационной безопасности Российской Федерации отмечено «вынужденное, в силу объективного отставания отечественной промышленности, использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств»[320].

Эксперты отмечают, что приведенная в Доктрине ситуация обусловлена целым рядом факторов и причин, возникших в последние два десятилетия при проведении реформ по переходу нашей страны к рыночным отношениям. Хотя следует отметить, что определенное отставание в информационно-коммуникационных технологиях от наиболее развитых государств начало проявляться еще в советский период.

К указанным факторам относят: самоустранение государства от управления информационно-коммуникационной отраслью экономики; низкие темпы развития этой отрасли; серьезная зависимость от внешних инвесторов; несогласованность в развитии магистральных сетей; высокий уровень зарубежного присутствия в акционерном капитале крупнейших компаний информационно-коммуникационной отрасли, причем во многих компаниях зарубежные партнеры обладают контрольными пакетами.

---

[320] Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации В.В. Путиным 9 сентября 2000 г., № Пр-1895 // URL.: http://www.rg.ru/OFICIAL/DOC/MIN_AND_VEDOM/MIM_BEZOP/DOCTR.SHTM. (дата обращения: 27.09.2013)

Специалисты особо подчеркивают, что существует сильнейшая зависимость развития и функционирования российских сетей связи от иностранных поставщиков. По некоторым оценкам, более 90% телекоммуникационного оборудования поступает из-за рубежа.

Следует признать несостоятельными иллюзии развития отечественного производства телекоммуникационного оборудования за счет развертывания производственных мощностей крупных зарубежных компаний («Alcatel», «Siemens», «Lucent Technologies», «Iskratel», «Nec», «Huawei») в России и предоставление им статуса российского производителя, который обеспечивает им льготные условия для захвата рынка. Как правило, все производства рассчитаны на выполнение самых элементарных завершающих производственных операций (сборка, упаковка)[321].

Отмеченные проблемы в развитии информационной сферы российского общества и телекоммуникационной отрасли отечественной экономики представляются особенно серьезными и имеющими принципиальный стратегический характер для дальнейшего развития нашей страны, если рассматривать их в аспекте глобального информационного противоборства. Для подобного обсуждения необходимо уточнить само понятие «глобальное информационное противоборство» (Рисунок 9).

[321] См.: О глобализации, информатизации и национальной безопасности России. Аналитический обзор / Под ред. С. А. Таразевича. СПб: Телерос, 2010. С. 40–43.

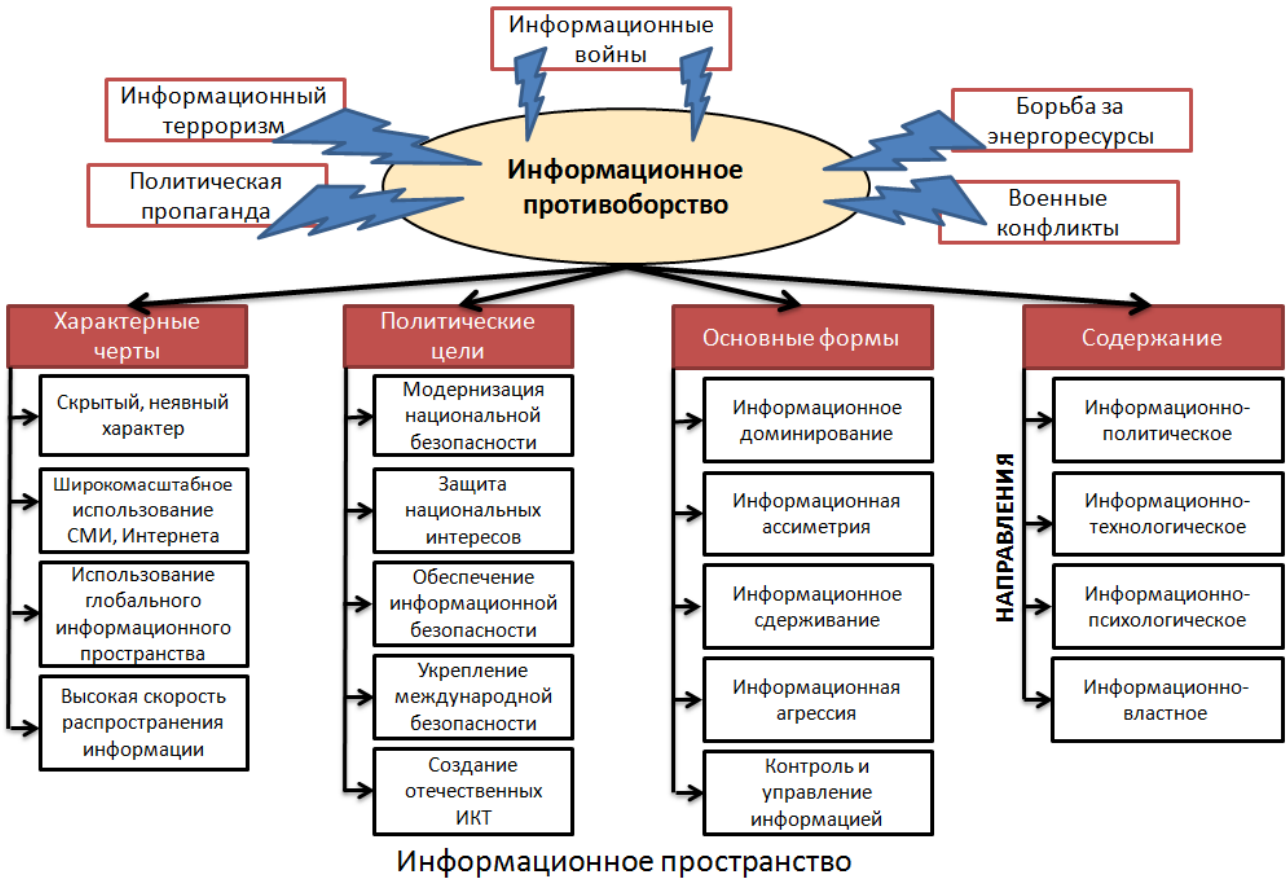


Рисунок 9 – Глобальный процесс информационного противоборства

Рассмотрим основные подходы к определению данной дефиниции, которые встречаются в отечественной литературе, посвященной изучаемой проблематике.

Исследователи, прежде всего, обращают внимание на субъекты, участвующие в противоборстве, и объекты, на которое осуществляется воздействие. При определении этих субъектов и объектов можно выделить два основных подхода: политический и социальный.

Так, А. И. Смирнов и его сотрудники анализируют изучаемый феномен под политическим углом зрения, рассматривая его как столкновение между различными государствами. Российские теоретики отмечают, информационное противоборство – это «форма межгосударственного противоборства, предусматривающая целенаправленное использование специально разработанных средств по воздействию на информационный ресурс противостоящей стороны и

защиты собственных ресурсов в интересах достижения поставленных политических и военных целей»[322].

Более широкую версию политического подхода при определении субъектов обсуждаемого противоборства предлагают Л. В. Воронцова и Д. Б. Фролов, которые пишут: «Информационное противоборство представляет собой совокупность взаимоотношений между субъектами мирового сообщества в рамках, которых данные субъекты, путем активного воздействия на информационную сферу друг друга, стремятся решать свои задачи в экономической, политической, военной или в иной областях, препятствуя при этом аналогичной деятельности противостоящей стороны»[323].

Таким образом, следует констатировать, что авторы первого подхода стремятся рассматривать информационное противоборство в рамках Вестфальской системы международных отношений, которая допускала участие в международном взаимодействии исключительно государств или их союзов и коалиций.

В данной связи изучаемый феномен понимается только как межгосударственное противоборство. Действительно: в современном мире наиболее мощными информационными потенциалами, способными вносить существенный (или решающий) вклад в глобальное противоборство, обладают наиболее индустриально развитые государства.

Однако, в последние десятилетия на мировой арене появились и другие достаточно активные участники международных политических процессов. На этой арене, наряду с государствами, выступают межправительственные и международные неправительственные организации, а также транс- и многонациональные корпорации, внутригосударственные регионы.

Пытаются вмешаться в мировые политические процессы, в том числе и информационное противоборство нелегальные структуры: международные

---

[322] Глобальная безопасность: инновационные методы анализа конфликтов / Под общ. Ред. А. И. Смирнова. М.: Общество «Знание» России, 2011. С. 242.

[323] Воронцова Л. В., Фролов Д. Б. История и современность информационного противоборства. М.: Горячая линия – Телеком, 2006. С. 3.

террористические и криминальные сети. Многие исследователи отмечают возрастание влияния на мировое сообщество глобальных медийных корпораций и транснациональных интернет-компаний.

Например, В. В. Фокина пишет: «В настоящее время присутствие СМИ в мировой политике дополняется интернет-сообществами и социальными сетями, что позволяет массированно воздействовать на мировое сообщество, используя не только линейные каналы подачи информации, но и вовлекая широкую общественность разных стран в процесс обсуждения актуальных мировых проблем.

Данного рода комплексное воздействие, несомненно, способно оказывать существенное влияние на процесс принятия политических решений в рамках мировой политики»[324].

Увеличение числа активных участников мировой политики получило отражение в указанном выше расширенном политическом подходе.

Объекты, которые подвергаются внешнему воздействию при информационном противоборстве, сторонники политического подхода располагают в информационной среде. К ним относятся как информационная сфера в целом, так и отдельные информационные ресурсы. Разрушение информационной инфраструктуры конкурирующего государства позволяет сначала достигнуть информационного превосходства, а затем – и доминирования в противоборстве на информационном геополитическом поле.

Второй из рассматриваемых нами подходов к трактовке понятия «информационное противоборство» акцентирует внимание на социальной стороне этого процесса.

В частности, А. В. Манойло, А. И. Петренко и Д. Б. Фролов отмечают: «Информационное противоборство – соперничество социальных систем в информационно-психологической сфере по поводу влияния на те или иные сферы социальных отношений и установления контроля над источниками стратегических ресурсов, в результате которого одни участники соперничества

[324] Фокина В. В. СМИ как акторы мировой политики // Вестник МГИМО-Университета. 2012. № 6 (27). С. 65.

получают преимущества, необходимые им для дальнейшего развития, а другие их утрачивают»[325].

Социальное измерение информационного противоборства также имеет большое значение для осмысления этого процесса. Оно позволяет показать, что данный процесс затрагивает фундаментальные основы общественного устройства и, при определенных обстоятельствах, может способствовать их разрушению. Объектами информационного воздействия, как показывают сторонники рассматриваемого подхода, могут стать жизненно важные сферы социальной жизни и стратегические ресурсы, обеспечивающие жизнедеятельность общества.

Каждое информационное противоборство на мировой арене преследует вполне определенные цели. В то же время, их анализ позволяет выявить цели более общего характера, присущие для глобального информационного противоборства в существующих условиях.

К этим целям следует отнести следующие:

− обеспечение национальной безопасности государства в глобальном информационном пространстве;

− защита и продвижение национальных интересов в информационной сфере;

− обеспечение информационной безопасности как важного элемента в системе национальной безопасности;

− укрепление международной информационной безопасности путем уменьшения возможностей для враждебного использования информационно-коммуникационных технологий в глобальном информационном пространстве.

Для достижения данных целей в процессе глобального информационного противоборства используются соответствующие способы и методы борьбы:

− информационное доминирование или достижение превосходства в информационном пространстве;

---

[325] См., например: Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны. М.: Горячая линия – Телеком. 2012. С. 478.

− информационная асимметрия в качестве базового принципа информационного воздействия, применяемая как ответ на внешнее влияние, так и при оказании воздействия на другую сторону информационного противоборства;

− информационное сдерживание как способ управления кризисными ситуациями в зонах конфликтов;

− внешний контроль информационного пространства государства и управление информационными процессами, осуществляемое из иностранных центров;

− информационная агрессия, в основе которой лежит незаконное осуществление одним государством информационного воздействия на информационное пространство другого государства, наносящего ущерб его суверенитету, политической независимости и жизнедеятельности в различных сферах;

− информационная война, которая «является наиболее острой формой информационного противоборства между государствами, осуществляемого насильственными средствами и способами воздействия на информационную сферу противника с целью решения стратегических задач. Сущность информационной войны в современный период состоит в скрытном управлении политическими, экономическими, военными и иными процессами государства-противника»[326].

Рассмотрим более подробно указанные выше способы и методы, применяемые в существующих условиях глобального информационного противоборства с учетом потребностей обеспечения национальной безопасности Российской Федерации в информационном измерении.

1) Информационное доминирование (или достижение превосходства в информационном пространстве) позволяет ведущим державам достигать политических целей на мировой арене, соответствующих защите и продвижению их национальных интересов, без применения вооруженной силы. Военные действия, как правило, связаны с достаточно большими политическими и

[326] Воронцова Л. В., Фролов Д. Б. Указ. соч. С. 80.

материальными издержками. Они могут наносить ущерб имиджу государства, которое прибегает к применению силы, особенно когда ее использование идет вразрез с нормами международного права и вызывает неоднозначные оценки в мировом сообществе.

Однако, информационное доминирование в глобальном информационном пространстве оказывает разнонаправленное и противоречивое влияние на внешнюю политику великих держав и мировые политические процессы. В ряде случаев такое доминирование не заменяет применение вооруженных сил, а, наоборот, создает условия для применения военной силы. Примером может служить вторжение США в Ирак в марте 2003 года.

Как известно, американская администрация не смогла получить поддержку Совета Безопасности ООН на применение силы в отношении указанной страны Среднего Востока. И все же США и Великобритания совершили вторжение в Ирак.

Принятие этого решения, нарушавшего нормы международного права, обострившего ситуацию в международном сообществе и оказавшего, в итоге, негативное влияние на внутри- и внешнеполитические процессы в Соединенных Штатах, а также способствовавшего, по мнению многих ведущих экспертов, поражению Республиканской партии на президентских выборах в 2008 году, было обусловлено рядом причин.

Первая группа таких причин имеет политическую природу. На рубеже 1990-х – начала 2000-х гг. американская политическая элита испытывала необычайный подъем, связанный с победой в «холодной войне», распадом СССР и фактической ликвидацией мировой социалистической системы. В этой элите господствовало убеждение, что наступил «Век Америки», что США теперь могут единолично править миром и создать под своим руководством глобальную либеральную империю.

Вторая группа причин имела информационно-пропагандистский характер. К этому времени США уже обладали мощнейшим идеологически-

пропагандистским комплексом и достигли превосходства в мировом информационном пространстве.

Это превосходство было связано с тем, что большинство крупнейших информационных агентств, медийных компаний и глобальных телевизионных сетей были американскими (в значительной степени находились под контролем США или под их влиянием). Под контролем США находился и набиравший силу Интернет. «На начало 2003 года подавляющее большинство системообразующих серверов (по некоторым данным, 9 из 13 самых крупных) находились на территории США»[327].

Массированная информационная кампания, опиравшаяся на недостоверные сведения о том, что Ирак якобы обладает оружием массового уничтожения (ОМУ) в итоге на какое-то время оказала благоприятное для американской администрации воздействие на общественное мнение в самой Америке и за ее рубежами.

В мае 2003 года Совет Безопасности ООН, не давший ранее согласие на вторжение в Ирак, фактически постфактум одобрил его. Одной из важных причин такого развития событий было мощное информационное наступление в поддержку действий американского правительства на Среднем Востоке.

По мнению руководителя Центра исследований внешнеполитического механизма США Института США и Канады РАН С. М. Самуйлова, развитие ситуации, связанной с вторжением в Ирак, наглядно показало «склонность значительной части политической элиты США, в первую очередь, принадлежащей к Республиканской партии (включая и руководителей разведывательных органов), к упрощенному черно-белому восприятию внешнего мира.

В рамках такого восприятия США всегда выступают воплощением «вселенского добра», а противоположная сторона – «всеобщего зла». Другими словами, сама специфика внешнеполитического сознания американцев

---

[327] Современные международные отношения и мировая политика / Отв. ред. А. В. Торкунов. М.: Просвещение: МГИМО, 2004. С. 228.

подталкивала и подталкивает руководителей внешнеполитических и разведывательных ведомств к преднамеренной демонизации противоположной стороны»[328].

Подобное упрощенное восприятие внешнего мира и преднамеренная демонизация своих оппонентов, в сочетании со стремлением американских руководящих кругов к информационному доминированию, создает определенные потенциальные угрозы для международной безопасности и национальной безопасности России, в первую очередь, в информационном измерении.

В наши дни американская сторона рассматривает информационно-пропагандистское обеспечение военных действий как важный элемент применения силы против других государств. Получают также широкое распространение кампании по оказанию давления на государства, не согласные с политикой Соединенных Штатов в том или в ином регионе (или по какой-либо проблеме мировой политики).

«Основными задачами при достижении информационного превосходства является «обрушивание на противника «целенаправленно препарированной» информации или просто дезинформации, а также ограничение его возможностей получать достоверные сведения о планах и намерениях США и их союзников.

Важной частью информационной войны является создание в собственной стране благоприятного общественного мнения вокруг осуществляемой операции. Спектр используемых средств варьируется от традиционной пропаганды и агитации до применения новейших технических средств»[329].

Информационное доминирование представляет собой сложный, многоаспектный процесс, затрагивающий основные сферы жизнедеятельности общества. Воздействие на жизненно важные стороны развития государства и общества связывает данный процесс непосредственно с проблемами обеспечения национальной безопасности.

---

[328] Самуйлов С. М. Вторжение США в Ирак // Свободная мысль. 2012. Июнь. №№ 3–4. С. 54.
[329] Современная мировая политика: Прикладной анализ / Отв. ред. А. Д. Богатуров. М.: Аспект-пресс, 2010. С. 222.

Сущностью процесса информационного доминирования (или превосходства) является сбор и распространение информации, что непосредственно обуславливает его связь с разведывательной и военной деятельностью. Информационное превосходство проявляется в мощном воздействии на общественное сознание, а через него, как и по другим каналам, осуществляется влияние на политические и на экономические процессы, деятельность средств массовой информации, поведение политических и бизнес-элит в государствах, на которые направлено информационное давление доминирующей державы.

В данной связи руководитель Центра проблем промышленной политики США ИСКРАН Е. А. Роговский пишет: «Информационное доминирование – вопрос комплексный (многоаспектный). С функционально-прикладной точки зрения в нем можно выделить составляющие, тесно связанные с национальной безопасностью, – военную и разведывательную (к которой примыкает экологический и метеорологический мониторинг), а также конкурентные преимущества бизнеса и информационное обеспечение средств массовой информации (СМИ)»[330].

В то же время, необходимо отметить, что полное информационное доминирование может быть достигнуто только с помощью физического разрушения или ликвидации информационных средств противоположной стороны, что может быть реально достигнуто только в ходе боевых действий. В современных условиях международных отношений следует говорить, за исключением зон вооруженных конфликтов (Ирак, Ливия, Сирия и так далее) о процессах достижения и поддержания информационного превосходства.

Как комплексный и многоаспектный процесс информационное превосходство связано с другими важными процессами и действиями в глобальном и региональном информационных пространствах. Рассмотрим их также более подробно.

---

[330] Роговский Е. А. Американская стратегия информационного преобладания // Россия и Америка в XXI в. Электронный научный журнал. 2009. № 3. URL: http://www.rusus.ru/?act=read&id=161. (дата обращения: 20.11.2013)

2) Информационная асимметрия представляет собой фундаментальный принцип информационного воздействия. Этот принцип может быть использован как стороной, осуществляющей информационное превосходство и стремящейся к информационном доминированию, так и стороной, стремящейся защититься от внешнего влияния в ходе информационного противоборства. Применение информационной асимметрии оказывает существенное влияние на формирование конфигурации информационного пространства современного государства.

Асимметрия (в греческом языке – asymmetria) означает неравномерность, несоразмерность. В применении к информационной асимметрии в современных исследованиях данного вопроса, это понятие применяют в нескольких смыслах.

Во-первых, асимметрия рассматривается как ситуация, в которой не существует общей базы для сравнения. В сфере информационной безопасности асимметрия может проявляться в качестве применения асимметричных информационных стратегий и появлении асимметричных угроз.

Информационное воздействие может сочетаться с применением действий из других сфер: например, в сочетании с политическими и военными кампаниями. В данном случае информационное пространство сопрягается с пространствами других видов деятельности: политическим, экономическим, военным и так далее.

Во-вторых, асимметрия используется для характеристики деятельности, которая осуществляется скрытно. Поскольку такого рода воздействия не замечаются и не фиксируются противоположной стороной, на них либо отсутствует какая-либо реакция, либо предпринимаются защитные действия общего порядка в пределах всего информационного поля государства.

Поскольку такие действия не носят целенаправленный характер и не фокусируются на асимметричной угрозе, они не могут обеспечить должную защиту (или такая защита отсутствует вообще).

В-третьих, асимметрия понимается как выборочный, ограниченный ответ на агрессивные информационные воздействия противника. Сегодня достаточно очевидно, что для сдерживания нет необходимости в поддержании паритета с возможным агрессором ни в количестве вооружений, ни в наносимом ущербе.

Достаточно сохранять возможность нанесения ему неприемлемого ущерба как ударными силами – в ответных действиях, так и оборонительными: в ходе отражения вооруженного нападения.

Выборочное сдерживание тем более оправдано в условиях, когда противники несопоставимы по военной и по экономической мощи. Для тотального сдерживания стороне, имеющей меньший военный потенциал, придется мобилизовать слишком большие ресурсы, тем самым подрывая другие составляющие национальной безопасности. Вот почему менее мощные в военном и в экономическом отношении страны вынуждены отказываться от попыток достижения и поддержания паритета с более сильными потенциальными противниками.

Данная стратегия применяется для обеспечения национальной безопасности. В современных условиях подобный подход целесообразен и для обеспечения информационной безопасности Российской Федерации.

3) Информационное сдерживание применяется как способ управления кризисными ситуациями в зонах конфликтов, а также используется и в других областях глобального информационного противоборства. В современных условиях глобального информационного общества структура военного сдерживания современного государства должна, наряду с системой вооружения для решения задачи сдерживания армии вероятного противника, включать систему средств и сил для информационного противоборства с экспансией возможного агрессора в информационной сфере.

Основными направлениями действий информационной системы, входящей в структуру военного сдерживания, являются решение следующих задач.

Во-первых, активное противодействие внешнему информационному давлению и атакам со стороны неприятеля с целью ослабить оборонный потенциал и нанести ущерб национальной безопасности государства. В Доктрине информационной безопасности Российской Федерации отмечено: «Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения

информационной безопасности Российской Федерации в сфере обороны, являются:

− все виды разведывательной деятельности зарубежных государств;

− информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети) со стороны вероятных противников;

− диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;

− деятельность иностранных политических, экономических и военных структур, направленная против интересов Российской Федерации в сфере обороны»[331].

Во-вторых, информационная компонента структуры военного сдерживания должна быть нацелена на достижение следующих целей:

− доведение до международного сообщества информации о наличии у нашей страны военного потенциала для сдерживания любого агрессора;

− информационное воздействие, направленное на создание ясного представления у военно-политического руководства и широких слоев общества государств потенциальных противников о неотвратимости нанесения по ним ответного удара с неприемлемым для них ущербом.

Существенное значение для рассмотрения вопроса об информационном сдерживании в условиях глобального противоборства имеет обращение к позиции американского военного руководства по этой проблеме. В Вооруженных Силах США информационным сдерживанием занимается так называемое Киберкомандование, которое входит в состав Стратегического командования (СТРАТКОМа).

В данной связи показательными могут быть выступления на слушаниях по вопросам финансирования американского Киберкомандования в Конгрессе США

[331] Доктрина информационной безопасности Российской Федерации // URL:http://www.rg.ru/OFICIAL/DOC/MIN_AND_VEDOM/MIM_BEZOP/DOCTR.SHTM. (дата обращения: 27.09.2013)

(2012 г.) командующего стратегическим командованием ВС США генерала Р. Келера и начальника Киберкомандования К. Александера.

Американские военные заявили «о необходимости разработки как наступательных, так и оборонительных средств информационного сдерживания. Генерал К. Александер отметил, что угрозы в киберпространстве исходят как от государств, так и от негосударственных акторов международных отношений, а также подтвердил положения принятой недавно киберстратегии о возможности «ответных действий на кибератаки любыми доступными средствами – экономическими, политическими, дипломатическими и даже военными»[332].

В то же время, некоторые эксперты полагают, что, принимая во внимание большое количество негосударственных акторов, обладающих серьезными информационными ресурсами, а также наличие значительного числа средств и способов информационной экспансии, применение политики сдерживания в глобальном информационном пространстве может оказаться достаточно неэффективным.

В контексте приведенных выше заявлений об ответных действиях по отражению кибератак любыми средствами угрожающе звучит заявление директора национальной разведки США Дж. Клэппера, сделанное также в Конгрессе Соединенных Штатов, на слушаниях по вопросам угроз национальной безопасности, о том, что «особую озабоченность в киберпространстве вызывают Россия и Китай»[333].

Необходимо подчеркнуть, что в американской стратегии развития киберпространства и военной стратегии кибербезопасности, в качестве одного из важнейших направлений информационной политики Соединенных Штатов рассматривается информационное сотрудничество. Определенное взаимодействие в этом направлении американская сторона предполагает осуществлять с нашей страной. Имеется уже первый опыт такого сотрудничества.

---

[332] Цит. по: Шариков П. А. В бой идут кибервойска // Независимое военное обозрение. 2012. 13 апреля. С. 4.
[333] Там же.

Внешний контроль информационного пространства государства и управление информационными процессами, осуществляемое из иностранных центров, имеют существенное значение в современном глобальном информационном противоборстве.

Эти способы противоборства осуществляются в завуалированной форме и представляют скрытое вмешательство в дела суверенного государства. Данный контроль и управление, как показывает практика, не ограничиваются информационным пространством, а стремятся проникнуть во все жизненно важные сферы жизнедеятельности государства.

«В недалеком прошлом основной вид конкуренции между общественно-политическими системами лежал в плоскости военных столкновений. Иные виды конкуренции между системами просматривались как вспомогательные и подготовительные. Информационная революция обеспечила свободный доступ как к географическому, так и социокультурному пространству государства из единого пространства информационных коммуникаций и предоставила широкий спектр методов воздействия на противника»[334].

В наши дни появляются технические возможности, которые могут быть подкреплены соответствующими финансовыми и материальными ресурсами для целенаправленного влияния на процесс принятия вероятным неприятелем принципиальных, в том числе и стратегических решений в политической, военной, экономической и других областях жизни государства и общества.

Такое воздействие осуществляется, в первую очередь, посредством манипулирования информационными потоками и ресурсами как на глобальном, так и на национальном уровнях. Например, «…меньший объем информации в глобальном пространстве об операции стран НАТО в Афганистане по сравнению с новостями, скажем, из Ирака, – отмечает А. Гумерский, – вовсе не говорит о том, что в Афганистане ничего не происходит или не происходит ничего,

[334] О глобализации, информатизации и национальной безопасности России. Аналитический обзор / Под ред. С. А. Таразевича. СПб.: Телерос, 2010. С. 26.

заслуживающего внимания. Просто дела натовской коалиции идут в этом регионе не так успешно, как планировалось»[335].

Причем, в зависимости от конкретной ситуации, потенциального противника могут, в независимости от его целей и желаний, искусственно погружать в информационный потоки, наносящие ему конкретный ущерб. Возможна и обратная ситуация: когда государство-конкурент может быть отстранено (или ограничено) в доступе к информационным ресурсам, необходимым для обеспечения его национальной безопасности, конкуренто- или жизнеспособности.

В данной связи А. В. Шевченко пишет: «В целях обеспечения информационной безопасности к критически важным относят объекты, системы и институты государства, целенаправленное воздействие на информационные ресурсы которых может иметь последствия, прямо затрагивающие национальную безопасность. Это, в частности, органы государственного управления, а также собственно управленческая информация, лица, принимающие властные решения, общественное мнение как специфическое состояние сознания и массовой психики»[336].

Особо критический характер имеет воздействие на массовое общественное сознание внешнего контроля и управления информационными потоками. В условиях демократических обществ мнение народных масс непосредственно учитывается при принятии ответственных внешне- и внутриполитических решений, поддержка конкретных политических действий правительства обществом способствует их успешной реализации; отрицательное отношение общественности к таким действиям может привести к их провалу и к осложнению ситуации в стране.

Таким образом, общественное мнение следует рассматривать как главный объект информационно-психологического воздействия, которое может реально содержать определенные угрозы национальной безопасности государства.

---

[335] Гумерский А. Управление международной информацией // Международные процессы. 2010. № 1. Том 8. С. 33.
[336] Шевченко А. В. Управление безопасностью информационных процессов. М.: Изд-во РАГС, 2009. С. 84.

Информационная агрессия представляет собой одну из форм активного информационного противоборства, нацеленную на нанесение конкретного ощутимого ущерба другому государству в важных для него сферах жизнедеятельности.

Как правило, информационная агрессия ограничена по масштабам применения информационного воздействия и локализована в геополитическом пространстве. Этот вид информационного противоборства ориентирован на достижение конкретных целей и обычно завершается после их достижения.

Информационная агрессия может выступать как самостоятельный вид глобального информационного противоборства, так и дополнять агрессивные действия, проводимые с помощью обычных вооруженных сил. Так, стремление Соединенных Штатов к глобальному доминированию и связанные с этим акции по применению силы к суверенным государствам широко поддерживаются американскими и лояльными США средствами массовой информации, имеющими, в ряде случаев, глобальные масштабы деятельности.

Последние десятилетия мирового развития дают много примеров подобного рода информационных агрессий. Воздушной войне НАТО против Югославии предшествовала информационно-пропагандистская кампания по обвинению сербской стороны в реальных и вымышленных военных преступлениях, а также сокрытию (или оправданию) аналогичных действий албанских сепаратистов.

Ввод войск НАТО в Афганистан предварялся широким распространением информации о причастности талибов к трагедии 11 сентября 2001 года и другим злодеяниям. Нападение США и Великобритании на Ирак весной 2003 года обосновывалось длительным и детальным освещением поисков в этой стране оружия массового уничтожения (ОМУ) (эти сведения, как выяснилось впоследствии, оказались дезинформацией).

Продвижение планов развертывания элементов третьего позиционного района глобальной американской системы ПРО в Восточной Европе, выдвинутых в середине 2000-х годов и не отмененные до сих пор, происходит на фоне регулярных обсуждений экспертами предположительных угроз ракетного

нападения на страны Запада со стороны Ирана и других «враждебных государств».

Давление на Иран, предпринимавшееся в этот же период, сопровождалось глобальной информационно-психологической кампанией по обвинению этой страны в стремлении овладеть технологиями производства ядерного оружия, агрессивными намерениями в отношении Израиля и некоторых других соседних стран.

Сегодня мы видим развертывание мощной дезинформационной кампании против Сирии, обвиняемой в намерениях использовать химическое оружие, нарушениях прав человека и тому подобное.

Информационная война представляет собой наиболее интенсивную форму глобального информационного противоборства. «Официально термин «информационная война» впервые был введен в оборот директивой Министерства обороны США DOOD 3600 от 21.12.1992 г. Современный тип войны широко обсуждается в печати; более того: поток оценок и характеристик вышел за узкие рамки военной печати»[337].

Под этим термином американские стратеги подразумевают «комплексное информационное воздействие на систему государственного и военного управления противника». Такое воздействие призвано обеспечивать развитие ситуации в важной для США стране (или регионе) в благоприятном для них направлении уже в мирное время.

Если дальнейшее политическое давление со стороны Америки на такую страну приводит к возникновению вооруженного конфликта, то развернутая информационная война должна привести к полному параличу всей структуры управления противника. Как отмечают специалисты, одновременно с наступательным воздействием, информационная война предполагает обеспечение надежной защиты национальной информационной инфраструктуры.

Г. Б. Корсаков справедливо отмечает: «Реализация положений концепции «информационной войны» означает перенос акцента противоборства с

[337] См.: Еляков А. Информационные технологии и современная война /Свободная мысль. № 1. Январь 2008. С. 182.

традиционных форм воздействия (огонь, удар, маневр) в информационно-интеллектуальную область – в процесс принятия решений. Основная цель такой войны – дезинтеграция и расчленение целостности управления группировкой противника на изолированные друг от друга, дезориентированные и неуправляемые элементы, и их последующий вывод из строя»[338].

Таким образом, информационная война имеет своей целью получение военно-стратегического преимущества над неприятелем благодаря более мощному информационному потенциалу. Осуществление информационной войны на практике реализуется посредством проведения информационных операций. Эти операции нацелены на манипулирование информацией для достижения и поддержания информационного превосходства над противником за счет решающего влияния на его информационную инфраструктуру при одновременной защите собственной.

Информационные операции осуществляются комплексно. Среди них выделяют как наступательные, так и оборонительные. Проведение информационных операций в рамках информационной войны ведет к обострению глобального информационного противоборства на мировой арене.

* * *

В заключение настоящей главы можно сделать некоторые общие выводы.

Во-первых, в наши дни достаточно наглядно в мировом развитии проявляется тренд хаотизации международных политических процессов, что ведет к формированию предпосылок для существенной трансформации всей мировой социально-политической структуры и, соответственно, принципов обеспечения международной безопасности.

Политические изменения в мировом сообществе сочетаются с революционными и не менее значимыми сдвигами в науке и технике, которые

[338] Корсаков Г. Б. Роль информационного оружия в военно-политической стратегии США // США – Канада. Экономика, политика, культура. Январь 2012. № 1. С. 49.

связаны, прежде всего, с колоссальным скачком в совершенствовании информационно-коммуникационных технологий.

Важнейшим результатом таких изменений является становление глобального информационного общества, которое представляет собой новый этап развития цивилизации.

Возникла тесная взаимосвязь между субъектами глобального информационного общества и акторами международных отношений. Эти акторы и субъекты взаимно дополняют друг друга, а часто в их качестве выступают одни и те же участники международных процессов. К ним следует отнести в первую очередь: государства, крупный бизнес, транснациональные медиакорпорации, гражданские институты, некоммерческие и неправительственные организации, транснациональные социальные сети, индивидуумов.

В связи с тем, что Россия непосредственно и широко представлена во всех основных группах участников глобального информационного общества, обеспечение национальной безопасности нашей страны напрямую связано с феноменом глобальной информационной безопасности.

В то же время, поддержание глобальной информационной безопасности в определенной мере зависит от действий Российской Федерации как общепризнанной мировой державы. Данная взаимосвязь повышает и конкретизирует роль международного фактора в обеспечении национальной безопасности нашей страны применительно к современным условиям.

Во-вторых, международный фактор играет значительную роль в создании угроз национальной безопасности нашей страны, исходящих из глобального информационного пространства. Эти угрозы связаны с: деятельностью глобальных и региональных СМИ; возникновением и активизацией частных PR-агентств, выполняющих задания по ведению подрывных операций против других стран в информационном пространстве; с сетевыми коммуникациями, которые составляют новую дополнительную структуру современного общества.

Непосредственно связаны с внешнеполитическими и международными аспектами деятельности нашего государства угрозы информационному

обеспечению государственной политики Российской Федерации. Международный фактор играет существенную роль в создании угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи.

В-третьих, вопросы обеспечения информационной безопасности в современном глобальном мире находятся в центре внимания внешней политики Российской Федерации. При этом наша страна выступает с важными инициативами по международно-правовому обеспечению глобальной информационной безопасности.

В данной связи российская сторона рассматривает возможное противоправное использование информационных технологий во всех сферах, где они применяются. Таким образом, под запрет (или под ограничение) подпадают как информационно-психологические операции, так и другие подобные виды враждебного воздействия. США стремятся свести проблемы глобальной информационной безопасности к вопросам предотвращения киберугроз.

В-четвертых, в условиях современного глобального мира традиционные геополитические факторы как военная мощь государства, его демографический потенциал, экологическое измерение дополняются информационным фактором как важным инструментом оказания влияния на международную политику и национальную безопасность.

Так, в результате внедрения в международные процессы информационных технологий возникли новые угрозы национальной безопасности России, имеющие геополитический характер. Эти угрозы требуют, для их изучения и осмысления, проведения соответствующего анализа с позиций современной геополитической теории.

При этом географическая среда и другие пространственные характеристики государств рассматриваются в тесной взаимосвязи с состоянием глобального, регионального и национального информационных пространств.

Статус государства в международном сообществе все больше начинает зависеть от его места и роли в мировом информационном пространстве, а также от его внешнеполитического информационного потенциала.

В глобальном информационном пространстве, которое тесно связано с мировым геополитическим пространством, разворачиваются следующие международные процессы: борьба за достижение информационного превосходства в процессе геополитической конкуренции между ведущими державами; проведение информационной политики по защите геополитических интересов конкретных государств; обеспечение информационной безопасности в рамках геополитических процессов.

В-пятых, информатизация современного международного сообщества протекает сегодня в тесной взаимосвязи с изменением и с усложнением геополитической структуры мира. Данный процесс способствует дальнейшей дифференциации внутри этой структуры, в том числе за счет формирования и развития глобального, регионального и национальных информационных пространств.

Геополитическая конкуренция между различными державами и другими субъектами международных отношений в этих пространствах обуславливает увеличение роли информационных ресурсов в современных геополитических процессах. Информационная мощь ведущих держав современного мира в некоторых случаях позволяет им реализовывать свои важные геополитические цели без применения силовых инструментов.

Одновременно развитие глобального информационного пространства, несомненно, способствует более широкому распространению принципа баланса интересов в обеспечение информационной безопасности в рамках геополитических процессов.

В-шестых, одним из основных направлений глобальной конкуренции в современном мире является противоборство в информационной сфере, важными сторонами которого следует рассматривать доступ к информационно-коммуникационной инфраструктуре, а также способность государства не только

использовать информационно-коммуникационные технологии, но быть в состоянии воспроизводить их.

Для глобального информационного противоборства присущи следующие цели: обеспечение национальной безопасности государства в глобальном информационном пространстве; защита и продвижение национальных интересов в информационной сфере; обеспечение информационной безопасности как важного элемента в системе национальной безопасности; укрепление международной информационной безопасности путем уменьшения возможностей для враждебного использования информационно-коммуникационных технологий в глобальном информационном пространстве.

В процессе глобального информационного противоборства используются такие способы и методы воздействия на противника, как информационное доминирование или достижение превосходства в информационном пространстве; информационная асимметрия как базовый принцип информационного воздействия; информационное сдерживание как способ управления кризисными ситуациями в зонах конфликтов; внешний контроль информационного пространства государства и управление информационными процессами, осуществляемое из иностранных центров; информационная агрессия; информационная война, которая «является наиболее острой формой информационного противоборства между государствами, осуществляемого насильственными средствами и способами воздействия на информационную сферу противника с целью решения стратегических задач».

5. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ В КОНТЕКСТЕ РЕГИОНАЛЬНОГО РАЗВИТИЯ

Вопросы, связанные с формированием и с обеспечением системы коллективной безопасности в информационной сфере на региональном уровне, в XXI веке актуальны как никогда. Возникла и продолжается острая борьба между государствами и группами государств за информационное превосходство в глобальном и региональном пространствах. Данная борьба затрагивает фундаментальные вопросы обеспечения суверенитета страны.

Президент России В. В. Путин, выступая на заседании Совета Безопасности РФ 22 июля 2014 года, заявил: «Суверенитет и территориальная целостность – фундаментальные, как я уже сказал, ценности. Речь идет об обеспечении независимости и единства нашего государства, надежной защите территории, конституционного строя, своевременной нейтрализации внутренних и внешних угроз. А в сегодняшнем мире их хватает.

Должен сразу отметить, что, разумеется, прямой военной угрозы суверенитету и территориальной целостности нашей страны, конечно, сегодня нет. Гарантия тому, прежде всего, – стратегический баланс сил в мире»[339].

В условиях продолжающихся мировых процессов, охвативших все основные сферы жизнедеятельности международного сообщества, информационно-телекоммуникационные технологии стали одним из важнейших политико-экономических, социальных и военных ресурсов, в том числе и на региональном уровне.

В связи с этим возникают новые угрозы, которые провоцируются США и странами Запада с использованием, в полной мере, возможностей информационного пространства, мировой сети Интернет, мгновенно распространяя информацию, направленную на подрыв национальной

[339] Заседание Совета Безопасности. 22 июля 2014 г. Москва. Кремль // http://state.kremlin.ru/news/46305/print. (дата обращения: 24.07.2014)

безопасности, прежде всего, России и других стран СНГ. Это проявляется во всех основных сферах жизнедеятельности общества:

− *экономической* – нарушение устойчивых экономических связей России внутри СНГ и с другими странами мирового сообщества путем введения санкций; порождение экономических кризисов с целью подрыва национальной экономической стабильности в финансовой, энергетической, космической, оборонно-промышленной и других отраслях;

− *политической* – целенаправленное доведение искаженной информации до мирового сообщества по вопросам проводимой Россией политики внутри страны и на международной арене. Это особенно характерно в связи с событиями, происходящими в Украине в последнее время;

− *военной* – введение в заблуждение стран мирового сообщества со стороны США относительно истинных причин создания многоэшелонированной системы ПРО, в том числе вблизи границ России; распространение Государственным департаментом США ложной информации о применении Вооруженных сил России во внутреннем вооруженном конфликте на территории Украины, широко используя при этом возможности современных информационно-коммуникационных технологий;

− *информационной* – активное использование современных ИКТ, глобального информационного пространства для внедрения в сознание граждан и общества чуждой идеологии, направленной на подрыв суверенитета России; политики нарушения устойчивости функционирования системы управления важными объектами промышленности в энергетике, на транспорте, в банковской сфере; проведении хакерских атак и внедрении вредоносных программных продуктов.

В данном контексте возможным становится следующее заключение: информационная безопасность в настоящее время является важнейшим компонентом национальной, региональной и международной безопасности. Отсюда вывод: политика информационной безопасности Российской Федерации на региональном уровне должна учитывать следующие факторы:

− информационная сфера стала системообразующей, и от ее состояния в значительной степени зависит уровень экономического, политического, военного и социального развития государства, общества и личности;

− значительный прогресс в развитии и внедрении новейших ИКТ и средств во все сферы жизнедеятельности общества повлек за собой и новые угрозы в информационной сфере, направленные на дестабилизацию национальной безопасности государства, и прежде всего – на постсоветском пространстве;

− анализ существующих и возможных угроз на национальном, региональном и международном уровнях показывает, что в современных условиях возникает опасность проявления кризисных ситуаций и совершения противоправных действий в отношении государственного суверенитета с применением современных ИКТ;

− возможный ущерб от реализации угроз в информационной сфере может оказать существенное влияние на информационную безопасность страны, снижая ее уровень, что, в конечном итоге, может подорвать устои национальной безопасности государства во всех сферах его жизнедеятельности и на всех уровнях, включая региональный.

5.1. Особенности формирования и реализации политики информационной безопасности в Евразийском регионе

За последнее время для разрешения спорных вопросов между государствами на региональном уровне (или, внутри страны, – на национальном) характерным становится фактор применения военной силы, а не использования путей переговоров и мирных соглашений.

Тон в этом задают США и их западные союзники. Печальными примерами такой политики стала агрессия режима Саакашвили против Южной Осетии в августе 2008 года, которая привела к большой трагедии на Кавказе, а также

развязанная весной 2014 года нынешним киевским режимом гражданская война против собственного народа на юго-востоке Украины.

Актуальным в данной связи является следующее заключение С. Б. Иванова: «Реальностью становится осуществление международных силовых операций вне традиционных военно-политических организаций и институтов. Военная сила все чаще применяется в рамках коалиций, сформированных на временной основе. Такая практика, вероятно, станет расширяться и в дальнейшем. Россия продолжает настаивать на строгом соблюдении норм международного права при формировании подобных коалиций и будет вступать в них только в том случае, если этого потребуют ее национальные интересы»[340].

На современном этапе, когда система геополитических отношений зачастую формируется заново, необходимость поиска новых подходов к оценке уровня обеспечения национальной безопасности всегда остается принципиально важной. На процесс обеспечения национальной безопасности в современном мире серьезное влияние оказывают изменения конфигурации международных отношений.

Такие изменения непосредственно затрагивают и нашу страну – Российскую Федерацию. После распада Советского Союза изменилось геополитическое положение России в мире и на Евразийском материке. Страна оказалась словно бы отодвинутой на северо-восток, в глубь Евразии. Таким образом, в конце прошлого века Россия лишилась ряда геополитических и геостратегических преимуществ, позволявших ей и ее союзникам на протяжении десятилетий осуществлять соответствующее своим интересам военно-политическое маневрирование.

Между Россией и ее основными торговыми партнерами в Европе образовался пояс так называемых «транзитных стран», через территорию которых теперь проходят российские грузопотоки, включая доставку углеводородов от мест их добычи к государствам-потребителям.

---

[340] Иванов С. Б. Вооруженные силы России и ее геополитические приоритеты//Россия в глобальной политике. 2004. № 1. С. 36

В диссертационном исследовании обращено внимание на особенности формирования и реализации информационного измерения политики национальной безопасности России на региональном уровне в рамках Евразийского пространства.

Содружество Независимых Государств (СНГ) – межгосударственное объединение, созданное на основе Соглашения о его создании, подписанного в 1991 году представителями трех республик бывшего СССР: России, Белоруссии и Украины.

В соответствии с Уставом СНГ, целями этого Содружества является развитие равноправного и взаимовыгодного сотрудничества народов и государств в области политики, экономики, культуры, образования, здравоохранения, охраны окружающий среды, науки, торговли, в гуманитарной и в иных областях; содействие широкому информационному обмену; добросовестное и неукоснительное соблюдение взаимных обязательств.

Устав СНГ был принят в 1993 году, однако Украиной он до сих пор так и не ратифицирован.

Основными институтами (консультативными и координирующими органами) СНГ являются: Совет глав государств Содружества, Совет глав правительств, Исполнительный секретариат СНГ, Межгосударственный экономический комитет, Экономический Суд СНГ, Межпарламентская Ассамблея государств – участников СНГ[341].

При образовании СНГ, в целях сохранения традиционной близости отдельных черт и понятийной основы законодательства ранее входивших в состав СССР государств, было принято решение о формировании в рамках Содружества системы модельного законодательства. Конвенцию о Межпарламентской Ассамблее государств (МПА) – участников Содружества Независимых Государств руководители стран СНГ подписали в 1995 году.

[341] См.: Косов Ю. В., Торопыгин А. В. Содружество Независимых Государств: Интеграция, парламентская дипломатия и конфликты. М.: Аспект-Пресс. 2012. С. 16-47.

МПА СНГ состоит из парламентских делегаций государств-участников и взаимодействует со всеми странами СНГ в сфере безопасности. Адаптируя международный опыт борьбы с угрозами безопасности к условиям государств Содружества, МПА СНГ разрабатывает для них типовые модельные законодательные акты и рекомендации. Эти документы не обладают обязательной юридической силой, однако наличие типовых моделей правового регулирования определенных отношений составляет потенциал для развития национальных систем законодательства в общем ключе. Благодаря их наличию создаются механизмы включения положений международных политико-правовых документов в национальные политико-правовые системы государств-участников.

Первыми актами СНГ, относящимися к информационной сфере, явились: Соглашение «О сотрудничестве в области информации» и Рекомендательный законодательный акт «О принципах регулирования информационных отношений в государствах МПА СНГ» (1993 год). В Рекомендательном акте, впервые в законодательстве СНГ, было использовано понятие «информационная безопасность», однако его конкретное содержание не раскрывалось[342].

Более чем за два десятилетия существования на постсоветском пространстве Содружества Независимых Государств разработано и принято большое число модельных и национальных нормативных политико-правовых актов. Необходимо отметить (это показала работа по составлению Словаря-справочника понятийного аппарата модельного законодательства государств – участников СНГ, выполненная в 2012 году при участии и под руководством автора диссертации), что для большинства этих актов характерно терминологическое многообразие и слабая определенность используемого понятийного аппарата[343].

Так, например, понятие «информационная безопасность» в международных политико-правовых актах МПА СНГ впервые получило свое определение в 2002

[342] Положение о разработке модельных законодательных актов и рекомендаций Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств: Постановление МПА СНГ от 23.11.2012 г. № 38-24.

[343] Словарь-справочник терминов и определений понятий модельного законодательства МПА СНГ. – СПб: Юридический центр Пресс. Серия «Юридические словари». 2012 г.

году (в Модельном законе «О международном информационном обмене») как «состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства».

В такой же трактовке это понятие было использовано и в «Стратегии сотрудничества государств – участников СНГ в сфере информатизации» (2006 год). Вместе с тем, «Концепция сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности», подписанная Советом глав государств в 2008 году, трактует понятие «информационная безопасность» уже как «состояние защищенности информационной сферы, формируемой, развиваемой и используемой с учетом жизненно важных интересов личности, общества и государства».

Набор терминов, используемых в «Концепции сотрудничества в сфере обеспечения информационной безопасности», характеризует задачи защиты информации; при этом основное внимание уделяется исключительно процессам хранения, обработки и передачи информации.

Аналогичную названной в «Концепции…» трактовку понятия «информационная безопасность» использует и «Стратегия сотрудничества государств – участников СНГ в построении и развитии информационного общества», утвержденная в 2012 году.

Отмеченное выше, по мнению автора, позволяет говорить о недостаточно целостной и последовательной информационной политике, осуществляющейся в рамках СНГ.

Комплексным планом мероприятий по реализации «Концепции сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности на 2008–2010 годы» была предусмотрена разработка «Рекомендаций по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности». С некоторым запозданием этот

вопрос нашел свое отражение в «Перспективном плане модельного законотворчества в СНГ на 2011–2015 годы».

Такой документ, носящий концептуальный характер, был подготовлен с участием автора, прошел экспертное обсуждение в парламентах государств-участников и был принят на 38-м пленарном заседании МПА СНГ (в 2012 году).

Целью разработки «Рекомендаций по совершенствованию и гармонизации законодательства в сфере информационной безопасности» явилось формулирование общих подходов для государств Содружества по ее правовому регулированию. Разработчики «Рекомендаций…» предложили опереться на трактовку понятия «информационная безопасность – состояние защищенности личности, общества, государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве», использованную в «Соглашении о сотрудничестве в области обеспечения международной информационной безопасности», заключенном в 2009 году между правительствами стран – участников Шанхайской организации сотрудничества.

В «Рекомендациях…» также были обоснованы предложения по изменению базового Модельного закона МПА СНГ «Об информатизации, информации и защите информации» и по разработке нового Модельного закона «Об объектах критически важных информационных технологий». Эти предложения были поддержаны Советом Федерации Федерального Собрания Российской Федерации и нашли отражение в обновленном перспективном плане законотворчества МПА СНГ на 2012–2015 годы.

Проект Модельного закона МПА СНГ «Об объектах критически важных информационных технологий» разрабатывается интернациональным коллективом российских и белорусских ученых при участии автора. Необходимость подготовки такого нормативного акта обусловлена увеличением числа критически важных объектов в системе информационно-коммуникационной инфраструктуры Содружества и отсутствием, в настоящее время, в большинстве стран данной организации нормативно закрепленных основ деятельности по обеспечению безопасности функционирования таких объектов.

Этим определяется важность установления общих, в рамках СНГ, подходов к содержанию административных процедур и перечню органов, их осуществляющих, а также к ожидаемому эффекту от реализации подобных процедур по недопущению деструктивного информационного воздействия на объекты критически важной инфраструктуры.

Под деструктивным информационным воздействием на автоматизированные системы управления производственными и технологическими процессами в разрабатываемом документе предлагается понимать несанкционированное информационное воздействие на элементы критической информационной инфраструктуры и обеспечивающие их взаимодействие информационно-телекоммуникационные сети.

Результатом подобного воздействия может стать возникновение аварий и катастроф, массовых беспорядков, длительных остановок транспорта, производственных или технологических процессов, дезорганизация работы органов власти, предприятий, организаций, нанесение материального ущерба в крупном размере, смерть или нанесения тяжкого вреда здоровью хотя бы одного человека и иные тяжелые последствия.

Примеры аварии на Саяно-Шушенской ГЭС (август 2009 года) и взрыв на Баксанской ГЭС (июль 2010 года) не оставляют сомнений в том, что деструктивное воздействие на элементы энергетической инфраструктуры национального хозяйственного комплекса способно привести к дезорганизации управления экономикой, угрозе безопасности жизнедеятельности населения региона и снижению уровня национальной безопасности в целом[344].

Одновременно с проектом Модельного закона разрабатывается примерный Модельный регламент реализации административных процедур, осуществляемых уполномоченными государственными органами в сфере обеспечения нормального функционирования и информационной безопасности объектов критически важной

[344] Вус М. А., Кучерявый М. М., Шакин Д. Н. Методологические проблемы обеспечения информационной безопасности критически важных объектов топливно-энергетического комплекса Российской Федерации // Информатизация и связь. 2012. № 7. С. 42.

инфраструктуры. В этой работе использован профессиональный опыт автора, приобретенный им в период работы в структуре ФСТЭК России.

Вместе с тем, проект Соглашения о сотрудничестве государств – участников СНГ в сфере обеспечения информационной безопасности (2013 год), изо всех государств СНГ подписали только шесть государств – членов Организации Договора о коллективной безопасности (ОДКБ). Таким образом, следует отметить, что более эффективной является деятельность по обеспечению информационной безопасности исключительно в рамках ОДКБ.

Договор о коллективной безопасности на постсоветском пространстве был подписан в 1992 году, но организация военно-технического сотрудничества появилась десятилетием позже. В настоящее время ОДКБ объединяет шесть независимых государств: Республику Армения, Республику Беларусь, Республику Казахстан, Кыргызскую Республику, Российскую Федерацию и Республику Таджикистан.

ОДКБ позиционирует себя как многофункциональная структура, которая занимается вопросами обеспечения безопасности входящих в нее стран, вопросами поддержания международной безопасности и стабильности. Использование сил и средств системы коллективной безопасности за пределами территории организации может осуществляться исключительно в интересах международной безопасности в соответствии с Уставом ООН и законодательством государств – членов ОДКБ[345].

Согласно Уставу Организации Договора о коллективной безопасности (принят в 2002 году, с изменениями от 2010 года), ее целями являются укрепление мира, международной и региональной безопасности и стабильности, защита, на коллективной основе, независимости, территориальной целостности и суверенитета государств-членов, «приоритет в достижении которых государства-члены отдают политическим средствам» (ст. 3 Устава ОДКБ).

В процессе формирования политики информационной безопасности на региональном уровне, по мнению автора, необходимо учитывать комплексный

[345] Об информатизации: Закон Кыргызской Республики от 08.10.1999 г. № 107.

характер данной проблематики, тесную связь информационной безопасности государств с их информационным же суверенитетом, взаимозависимость государственной политики информационного суверенитета и национальной безопасности ОДКБ.

В соответствии с Уставом ОДКБ, государства – ее члены принимают меры по развитию договорно-правовой базы, регламентирующей функционирование системы коллективной безопасности, по гармонизации национального законодательства, по вопросам обороны, военного строительства и безопасности. В качестве одного из основных направлений создания системы коллективной безопасности государства – члены ОДКБ рассматривают сближение основных положений законодательных актов в области обороны и безопасности.

«Концепция коллективной безопасности государств – участников Договора о коллективной безопасности» представляет собой совокупность взглядов стран данной организации на предотвращение и на устранение угрозы миру, совместную защиту от агрессии, обеспечение их суверенитета и территориальной целостности.

Эта «Концепция…» закрепляет приверженность стран Договора целям предотвращения войн и вооруженных конфликтов, устранению их из системы международных отношений, созданию условий для всестороннего развития личности, общества и государства на базе идеалов гуманизма, демократии и всеобщей безопасности.

В качестве источников военной опасности в названной «Концепции…» указаны попытки вмешательства извне во внутренние дела государств, стремление дестабилизации их внутриполитической обстановки, международный терроризм и политика шантажа. Сегодня подобные угрозы во многом реализуются через информационную сферу. Военная, экономическая, политическая и информационная безопасность тесно взаимосвязаны.

Информационные технологии уже стали одним из важнейших политико-экономических и военных ресурсов. В мирное время военную угрозу национальным интересам государства создает, прежде всего, разведывательная

деятельность иностранных государств в Глобальном информационном пространстве. При этом основную опасность представляют не сами разведывательные космические и наземные системы, осуществляющие сбор информации о состоянии различных объектов, группировок войск и условий возможных военных действий и не полеты иностранной разведывательной авиации вблизи государственных границ России.

Главная угроза заключается в том, что такие силы, средства и действия являются элементами Глобальной информационной сети. Подобная информационная сеть представляет собой материальную основу так называемой «сетецентрической» (по американской терминологии), или информационной (по принятой в Генеральном штабе Вооруженных сил РФ терминологии) войны[346].

Под информационной войной понимается «противоборство между государствами в информационном пространстве с целью нанести ущерб информационным системам, процессам и ресурсам, критически важным структурам (информационно-техническая война), подрыва политической и социальной систем, а также массированной психологической обработки личного состава войск и населения с целью дестабилизировать общество и государство (информационно-психологическая война)».[347]

При этом информационная война рассматривается не как обособленные действия, а как интеграция всех форм и способов вооруженной борьбы, при которой происходит значительное сокращение привлекаемых сил и средств за счет повышения информационных возможностей.

Ее суть заключается в том, что войска достигают информационного превосходства, под которым понимается как поступление информации в большем

---

[346] См.: Арапова Н. П. Социально-информационный подход в теории информационных войн: дис. ... канд. полит. наук: 10.01.10. М.: 2003; Гордиенко Д. В. Информационное противоборство в военных конфликтах / В кн. Актуальные проблемы информационного противоборства. М:, 2000; Гриняев С. Н. Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. Минск: Харвест. 2004; Попов В. Д. Тайны информационной политики. М.: Изд-во РАГС. 2003; Цыгичко В. Н., Смолян Г. Л., Черешкин Д. С. Информационное оружие как геополитический фактор и инструмент силовой политики. - М.: Институт системного анализа РАН. 1997.

[347] Война и мир в терминах и определениях. Под ред. Д. О. Рогозина. – М.: 2004. – С. 75.

количестве, так и повышение степени доступа к ней мелких звеньев системы и, как следствие, углубление понимания ситуации на поле боя.

Это становится возможным в результате доступа географически разбросанных войск к Единой информационной системе. При этом синхронизация их действий достигается уже не за счет централизованного управления, а за счет своевременной реакции этих войск на изменение обстановки.

Для лишения возможного противника заблаговременно накопленной информации, а также для минимизации наносимого в результате ведения разведки ущерба уже в мирное время должно осуществляться противодействие видовой и радиоэлектронной разведкам иностранных государств, которая ведется космическими и воздушными разведывательными системами, а также системами двойного назначения. Некоторые исследователи понимают информационное противоборство в мирное время в более широком масштабе.

Такой подход включает в данное противоборство не только военные задачи, но также вопросы военно-политического и геополитического характера. Он направлен на решение задачи сдерживания в мирное время потенциального агрессора от попыток вооруженного нападения на нашу страну.

Например, В. М. Буренок, в данной связи, пишет: «…система информационного противоборства основной задачей должна иметь формирование у руководства и общества стран – потенциальных агрессоров стойкого убеждения о недопустимости агрессии по причине нанесения по ним ответного удара с неприемлемым ущербом. Для этих целей информация о возможностях системы вооружения для решения задач сдерживания и способах ее применения (способах сдерживания) должна широко освещаться в средствах массовых коммуникаций. Речь, безусловно, не должна идти об исключительно пропагандистских мероприятиях – информационные действия должны регулярно подкрепляться

демонстрацией возможностей образцов вооружения, входящих в систему сдерживания»[348].

Информационная сфера – весьма чувствительный фактор жизнедеятельности общества. Повсеместно и объективно растут техногенные факторы и связанная с этим уязвимость.

«Программа совместных действий государств – членов ОДКБ по формированию системы информационной безопасности» была принята в 2008 году. В формате ОДКБ существует согласие относительно того, что под информационной безопасностью понимается состояние защищенности личности, общества, государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве[349].

В 2010 году обеспечение информационной безопасности как важное направление сотрудничества было закреплено в Уставе ОДКБ. Ст. 8 Устава ОДКБ гласит: «Государства-члены взаимодействуют в сферах охраны государственных границ, обмена информацией, информационной безопасности, защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, а также от опасностей, возникающих при ведении или вследствие военных действий».

В том же году Совет коллективной безопасности ОДКБ утвердил «Положение о сотрудничестве государств – членов ОДКБ в сфере информационной безопасности». В соответствии с этим «Положением…», в формате Организации определены национальные координирующие органы в сфере информационной безопасности.

Первым опытом скоординированной борьбы с киберпреступностью в масштабах ОДКБ явилась операция «ПРОКСИ» (противодействие криминалу в информационной сфере). Как сообщалось в печати, при ее проведении, в результате совместных действий в национальных сегментах интернет-

---

[348] Буренок В. М. Военная безопасность России – проблемы и решения // Воздушно-космическая оборона. 2008. № 3. – С. 56.

[349] Законодательство государств – членов ОДКБ в сфере обеспечения информационной безопасности: опыт, проблемы и перспективы гармонизации. Материалы международной научно-практической конференции (Санкт-Петербург, 28.11.2013). – СПб: Секретариат Совета МПА СНГ. 2014.

пространства, были выявлены тысячи ресурсов, использовавшихся для распространения информации, наносящей политический ущерб государственным и союзническим интересам. Во время известных событий в Киргизии (2010 год), например, было выявлено немалое число сайтов, которые использовались для разжигания межнациональной вражды. К таким ресурсам применялись ограничительные меры законодательного характера.

В 2011 году Советом коллективной безопасности ОДКБ был разработан и утвержден «Перечень мероприятий, направленных на формирование системы обеспечения информационной безопасности в интересах ОДКБ». В этой связи особую актуальность приобретают вопросы по формированию активной и согласованной политики государств для развития общего информационного пространства, создание совместного потенциала по противодействию информационным угрозам, правам и свободам граждан, интересам общества и суверенитета государства, защищенности информационных ресурсов и коммуникаций, органов власти и управления ОДКБ.

Совет коллективной безопасности ОДКБ утвердил основные направления развития военной составляющей организации до 2020 года, предусматривающие, в частности, развитие Единого информационно-программного пространства для ведения регулярного обмена информацией и совместного мониторинга.

В функции ОДКБ, кроме конкретных мероприятий, связанных с обеспечением безопасности государств, входят и задачи по анализу обстановки, рисков и угроз, а также выработки превентивных мер, которые не позволяли бы обостряться этим вызовам. Динамика развития ОДКБ дает основание говорить о будущем организации как мощного защитного «зонтика» безопасности для Евразийского союза.

Важнейшим направлением деятельности ОДКБ является гуманитарное сотрудничество и использование технологий так называемой «мягкой силы» для содействия созданию в Евразии среды безопасности, направленной на развитие национальных культур, межнациональных и межрегиональных культурных связей, поддержку взаимоуважения народов всех стран, возрождение и

сохранение культурно-нравственных ценностей, укрепление духовного единства народов Евразии.

В 2013 году была создана Аналитическая Ассоциация ОДКБ, объединяющая более 30 ведущих информационно-аналитических и социологических структур изо всех стран ОДКБ. Она предназначена для разработки мероприятий и стратегии скоординированной информационной политики, информационно-аналитической поддержки, налаживания деловых контактов, обмена информацией, проведения экспертного и ситуационного анализа и для более тесного взаимодействия сторон по формированию системы информационной безопасности государств – членов ОДКБ.

Под системой информационной безопасности в политических и правовых документах ОДКБ понимается комплекс мер правового, политического, организационного, кадрового, финансового, научно-технического и социального характера, нацеленных на обеспечение информационной безопасности организации.

Информационная сфера все более превращается в арену для международного, межрегионального и межгосударственного соперничества, острейшей конкуренции в бизнесе, противоправных действий криминальных структур. Крайними формами разрешения возникающих при этом конфликтов являются информационные и информационно-психологические войны, а также информационный терроризм. Все это создает опасные угрозы информационным национальным интересам ОДКБ.

Важнейшая составляющая деятельности органов власти стран ОДКБ по регулированию политических, экономических, социальных, военных и других отношений в информационной сфере определяется информационной политикой государств.

Информационная политика представляет собой деятельность органов власти государств – членов ОДКБ по формированию единых взглядов, определению основных направлений и реализации системы мер, отражающих интересы ОДКБ в информационной сфере.

Практическая реализация информационной политики в современных условиях требует широкой психологической кампании по поддержке ее основных положений в общественном мнении.

Традиционно ранее, на протяжении многих лет, информационная политика охватывала, главным образом, проблемы, связанные с деятельностью средств массовой информации (СМИ). За последние годы содержание этой политики значительно расширилось: ведущие мировые государства включили в нее развитие телекоммуникаций, информационных систем, средств и ресурсов, защиту гарантированных конституцией страны прав граждан и организаций на общедоступную информацию, а также соответствующие аспекты обеспечения информационной безопасности личности, общества и государства.

К основным стратегическим целям государственной информационной политики следует отнести:

1) обеспечение информационной безопасности и условий для повышения эффективности государственного управления;

2) создание условий для обеспечения конституционных прав и свобод человека в информационной сфере, сохранения и укрепления нравственных ценностей общества, традиций патриотизма и гуманизма, приумножение культурного и научного потенциала и формирование информационной культуры населения;

3) превращение региональных информационных ресурсов в стратегический ресурс устойчивого и поступательного развития и создание условий для гармоничного вхождения в современную мировую экономику на основе кооперации и информационной открытости – интеграции в международную систему разделения труда и обменов в информационной сфере.

Достижение целей информационной политики обеспечивается решением целого комплекса стратегических задач. При этом основными задачами являются:

– содействие формированию современной информационно-коммуникационной инфраструктуры и информационных ресурсов;

– создание условий для максимального использования и увеличения

интеллектуального и кадрового потенциала;

– формирование нормативно-правовой базы, регулирующей общественные отношения в информационной сфере;

– содействие формированию единой информационной среды науки и образования;

– обеспечение условий для стимулирования науки и производства, поддержки научных исследований в области развития и применения ИКТ и технологий;

– содействие развитию и обновлению всех сфер жизнедеятельности на базе широкого использования информационно-коммуникационной техники и технологий и др.

Решение основных задач государственной информационной политики осуществляется посредством оказания различных управляющих воздействий на основные объекты информационной среды, объекты информационной политики. Таковыми являются: информационные ресурсы и информационно-телекоммуникационная инфраструктура; информационные и телекоммуникационные технологии, системы и средства их реализации; производство и потребление средств информатизации, информационных продуктов и услуг.

В рамках последнего направления ведется работа по завершению процесса согласования, подписания и последующей ратификации «Протокола о взаимодействии государств – членов ОДКБ по противодействию преступной деятельности в информационной сфере» и согласование других предложений, носящих закрытый характер. Это направление работы относится, прежде всего, к вопросам координации сотрудничества по киберинцидентам.

Прогрессирующие сегодня компьютерная преступность и кибертерроризм представляют особую общественную национальную и международную опасность. В этой связи актуальна проблема соотношения силовых и политических средств противодействия кибертерроризму.

С указанным направлением работы тесно связано также предотвращение несанкционированного доступа к информации ограниченного распространения, имеющей значение для обеспечения целей коллективной безопасности. В аспекте военно-технического сотрудничества чрезвычайно актуальны вопросы защиты государственных секретов организации.

Правовые аспекты защиты государственных секретов в ОДКБ регламентированы «Соглашением о взаимном обеспечении сохранности секретной информации в рамках Организации Договора о коллективной безопасности», заключенном еще в 2004 году.

С 2010 года при участии автора проводятся научно-исследовательские работы в целях сближения законодательства стран ОДКБ по вопросам государственной тайны. Итогом этих работ стали принятые ПА ОДКБ «Рекомендации по сближению и гармонизации законодательства государств – членов ОДКБ в сфере защиты государственных секретов» и «Глоссарий основных понятий законодательства о государственной тайне государств – членов ОДКБ».

До настоящего времени на постсоветском пространстве не выработаны единые взгляды на понятия и категории информационной безопасности, не выстроена иерархическая система субъектов (сил) обеспечения информационно-коммуникационной безопасности, что замедляет деятельность органов данной организации по выработке единой законодательной базы.

Автором в ходе проведенного диссертационного исследования выработаны и предлагаются следующие направления сближения законодательства в информационно-политической сфере.

Во-первых, определение основных направлений по обустройству Единого безопасного информационного пространства как объединенного сегмента информационных пространств ОДКБ. Указанное направление потребует решения следующих задач: организации обеспечения информационной безопасности, защиты Единого информационного пространства, защиты информационных ресурсов, противодействия преступлениям в информационной сфере (в том числе информационному терроризму), обеспечения безопасности информационно-

коммуникационной инфраструктуры, информационного обеспечения реализации государственной политики.

Во-вторых, сближение и гармонизация законодательства стран ОДКБ, для чего необходимы: проработка единого понятийного аппарата, определение, определение основных угроз информационной безопасности, выработка концептуальных мер правового и политического обеспечения информационной безопасности по каждому аспекту, разработка системы организационных мер обеспечения информационной безопасности, совершенствование правового и политического обеспечения информационной безопасности на национальном уровне, гармонизация системы мер политико-правового обеспечения информационной безопасности на международном (региональном) уровне.

Рациональным представляется приведение национального законодательства государств – членов ОДКБ к единому стандарту и нормативной классификации информационных отношений, достижение которых на национальном уровне будет свидетельствовать о Едином информационном пространстве и единой инфоструктуре.

Автором предлагается введение единого стандарта и нормативной классификации, которые должны включать:

− документ стратегического планирования, определяющий цель и задачи обеспечения информационной безопасности;

− унифицированный, в рамках ОДКБ, понятийный аппарат в сфере обеспечения информационной безопасности;

− систему правовых предписаний и запретов, определяющих правила безопасного поведения в информационно-коммуникационной сфере;

− политико-правовой регламент по предотвращению криминальных действий в области информационно-коммуникационной сферы.

Сближение и гармонизацию законодательства стран Организации представляется рациональным осуществлять «сверху вниз»: от международного акта – к национальным, поскольку существующие структуры национальных политико-правовых систем в области информационной безопасности не могут

быть взяты за эталон формирования единой системы в рамках ОДКБ. Реализация такой задачи потребует эффективного механизма совершенствования нормативно-правовой базы и более детальной проработки модельного и национальных законодательств.

Таким образом, практически полезной представляется деятельность ПА ОДКБ по разработке «Концепции сотрудничества государств – членов ОДКБ по противодействию современным угрозам в информационной сфере» и «Соглашения о сотрудничестве государств – членов ОДКБ по организации межгосударственного обмена информацией в сфере обеспечения информационной безопасности».

Для достижения столь масштабных целей потребуются определенность и однозначность понятийного аппарата. Органам власти и управления, субъектам хозяйственной деятельности, физическим и юридическим лицам различных государств необходимы сведения, основанные на едином понимании предметов и явлений информационного пространства, регулируемого законодательными положениями.

Для эффективного взаимодействия и сотрудничества необходима развитая система терминов и понятий, их определений; ее закрепление в нормативных актах и в общественном обращении, а также правовое толкование понятийного аппарата в повседневной практике. Планами Экспертного совета Регионального содружества связи и Экспертно-консультативного совета при Парламентской Ассамблее Организации Договора о коллективной безопасности предусмотрена разработка глоссариев в области информационной безопасности.

До недавнего времени терминология по информационной безопасности помещалась в универсальные словари по информатике. Сегодня же информационная безопасность перестала быть только технической дисциплиной, частью информатики. Формирование системы современной терминологии информационной безопасности как международной системы терминов, понятий и их определений является актуальной задачей и требует для ее решения

использование достижений многих разноплановых наук: политики, правоведения, социологии, психологии, теории информации, кибернетики и др.

Учитывая актуальность такой задачи, коллективом специалистов при участии автора была предпринята попытка, на основе анализа доктринальных положений международно-правовых документов и норм национального законодательства стран ОДКБ, сформировать общий понятийный аппарат сферы информационной безопасности для целей Парламентской Ассамблеи, на который можно было бы опереться в последующем: при разработке нормативных и методических документов по информационной безопасности в рамках ОДКБ.

Такая работа успешно завершена. В 2014 году, при непосредственном участии и под редакцией автора, подготовлен и издан «Словарь-справочник по информационной безопасности для Парламентской Ассамблеи ОДКБ», включающий 163 лексические единицы легальных понятий с их определениями[350].

5.2. Совершенствование политики информационной безопасности в регионе (на опыте и примерах Северо-Западного федерального округа)

В XXI веке регионы Российской Федерации в полной мере включились в процесс формирования национального информационного пространства, подтвердив, тем самым, общую тенденцию мирового развития по созданию глобальной информационной среды. «Информационно-коммуникационные процессы, которые развертываются на международном уровне, носят весьма противоречивый характер. Они могут способствовать развитию сотрудничества между странами и народами; в то же время, они очень часто приобретают характер информационно-психологических войн»[351].

---

[350] Словарь-справочник по информационной безопасности для Парламентской Ассамблеи ОДКБ/ Под общ. ред. М. А. Вуса и М. М. Кучерявого. – СПб: СПИИРАН. 2014.

[351] Информационное общество и международные отношения / Под ред К. А. Панцырева. СПб: Изд-во СПбГУ. 2014. С. 14

В качестве таких регионов, исходя из целей и задач диссертационного исследования, целесообразно рассматривать федеральные округа. Информационно-телекоммуникационные средства и технологии, используемые в регионе, оказывают мощное влияние и определяют основные направления дальнейшего развития всех сторон жизнедеятельности входящих в него субъектов Российской Федерации. Автором изучены данные процессы на примере Северо-Западного федерального округа (СЗФО).

Основными факторами, влияющими на необходимость повышения внимания к вопросам информационной безопасности в округе, являются:

− геостратегическое положение СЗФО, заключающееся в соприкосновении с государствами – членами НАТО, наличием общих сухопутных и морских границ, расположением обособленного субъекта Российской Федерации (Калининградской области), не имеющего общей внутренней территориальной связи с другими регионами округа.

В Докладе Российского института стратегических исследований «Приграничные связи: ресурс евразийской интеграции и межгосударственного сотрудничества России» Калининградская область определена как «российский анклав в жестких объятиях «мягкой силы» Евросоюза»[352];

− расположение в пределах округа значительного числа совместных предприятий (в том числе со странами дальнего зарубежья), генеральных консульств, иностранных торговых представительств и банков;

− использование в органах власти и управления местного и регионального уровней информационных систем, накапливающих и передающих большие объемы информации, в том числе посредством сети Интернет. Возрастание риска и опасности несанкционированных и непреднамеренных воздействий на информацию в этих системах может привести к непредсказуемым экономическим и социальным взрывам в обществе, связанным с нарушениями режимов

[352] Доклад РИСИ «Приграничные связи: ресурс евразийской интеграции и межгосударственного сотрудничества России» // Проблемы национальной стратегии. 2014 . Вып. 1. С. 26.

безопасности информации в кредитно-финансовых учреждениях, системах управления экологически опасными производствами, транспортом, энергетикой;

− наличие и функционирование в органах власти всех уровней, организациях и предприятиях информационно-коммуникационных средств зарубежного производства, не сертифицированных по требованиям безопасности информации, что приводит к возрастанию зависимости результатов деятельности данных структур от достоверности используемой ими информации;

− возрастание информационных угроз в отношении органов власти и организаций, а также рост числа преступлений с использованием новых информационных технологий (пропаганда терроризма, разжигание межнациональной и межконфессиональной вражды, подстрекательство к насилию и нарушению общественного порядка, попытки деструктивного воздействия на системы управления транспортом, энергетикой, банковской сферой, распространение вредоносных программ);

− формирование государственных информационных ресурсов, находящихся в ведении субъектов Российской Федерации, организаций и граждан, необходимость защиты этих ресурсов от противоправных действий.

Процесс совершенствования политики информационной безопасности, с учетом особенностей развития и географического положения СЗФО, обуславливается решением следующих основных задач:

− совершенствование и развитие государственного регулирования политики информационной безопасности в органах государственной власти субъектов Российской Федерации, территориальных органах федеральных органов исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления и в организациях;

− анализ существующих и перспективных угроз информационной безопасности объектам округа, а также использование иностранных технических средств наблюдения и контроля в соответствии с международными договорами Российской Федерации на его территории;

− определение основных направлений политики совершенствования информационной безопасности в регионе: таких, как информационно-технологическая, информационно-психологическая и информационно-политическая. Каждое из направлений имеет собственный предмет исследования – это информационная безопасность на региональном и местном уровнях. Их объединяет то, что вышеупомянутая политика осуществляется в условиях «информационного господства» сети Интернет;

− организация и координация деятельности всех элементов государственной системы противодействия техническим разведкам и технической защиты информации на всех объектах округа;

− развитие системы информационной безопасности по противодействию техническим разведкам и недопущением деструктивного вмешательства в структуры технологического управления производством на объектах оборонно-промышленного комплекса;

− оказание методической помощи высшим учебным заведениям округа в организации деятельности по подготовке специалистов в области информационной безопасности.

Автор диссертационного исследования принимает непосредственное участие в работе по совершенствованию политики информационной безопасности в СЗФО, являясь заместителем председателя постоянно действующего Межведомственного совета по защите информации, деятельность которого координируется полномочным представителем Президента Российской Федерации в Северо-Западном федеральном округе.

Деятельность Совета направлена на проведение политики государственного регулирования в области информационной безопасности в округе путем выработки и доведения рекомендаций, обязательных для исполнения (рис. 10):

на *межрегиональном уровне* – территориальными органами федеральных органов исполнительной власти и подведомственными им организациями, образовательными учреждениями по подготовке специалистов в области информационной безопасности;

на *региональном уровне* – законодательными органами государственной власти, исполнительными органами государственной власти и подведомственными им организациями;

на *местном уровне* – органами местного самоуправления и подведомственными им организациями;

на *всех уровнях* – организациями оборонно-промышленного комплекса в области судостроения, авиастроения, космической, обычных вооружений, боеприпасов, специальной химии, систем управления войсками и оружием.

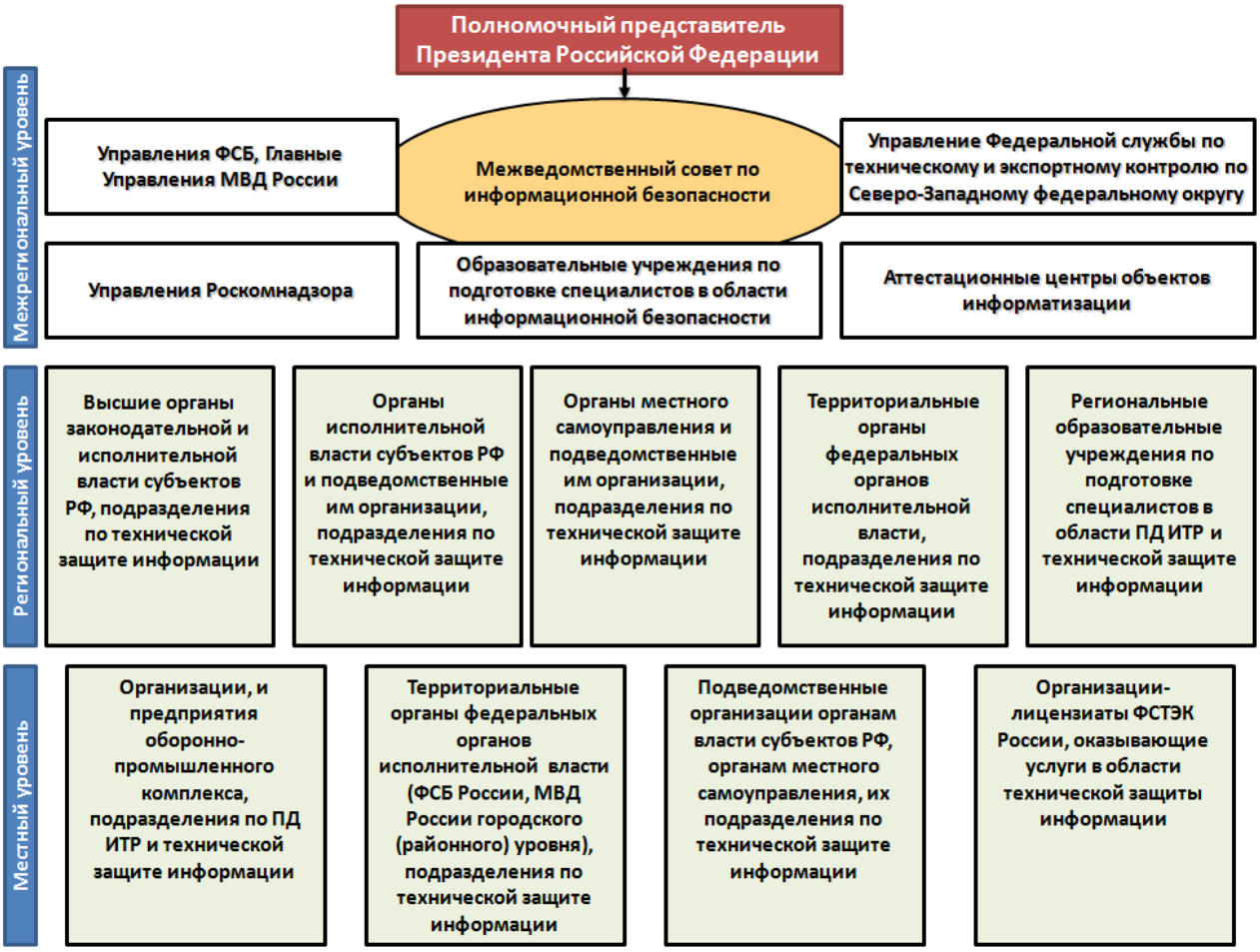


Рисунок 10. Система защиты информации в Северо-Западном федеральном округе

Политика информационной безопасности в СЗФО основывается на исполнении требований основных документов, и прежде всего «Доктрины информационной безопасности» 2000 года, «Стратегии национальной

безопасности» 2009 года, Указа Президента Российской Федерации от 12 мая 2009 года «О стратегии национальной безопасности Российской Федерации до 2020 года» и Федерального закона «Об информации, информационных технологиях и о защите информации» 2006 года и др.

Государственное регулирование в области обеспечения безопасности информации осуществляется по следующим направлениям: определение информационных ресурсов, подлежащих защите; установление требований по защите информационных ресурсов, механизмов реализации этих требований и предотвращение противоправных деяний в инфосфере.

В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации», руководителям органов власти и организаций предписано постоянно обеспечивать надлежащую защиту всех государственных информационных ресурсов: как имеющих ограничения в доступе к ним, так и открытых общедоступных.

При этом защита информации предполагает обеспечение заданных характеристик безопасности информации: ее целостности и доступности для открытой и общедоступной информации, а для информации с ограниченным доступом – еще и конфиденциальности.

Организация управлением деятельностью органов власти по реализации государственной политики в области безопасности информации осуществляется полномочным представителем Президента Российской Федерации в Северо-Западном федеральном округе через работу Межведомственного совета по защите информации. Структурная схема системы организации информационной безопасности в округе представлена на рис. 11.

Таким образом, приоритетным направлением государственного регулирования политики информационной безопасности в округе является деятельность всех структур по построению информационного общества с усилением внимания по защите информационных ресурсов на всех уровнях.

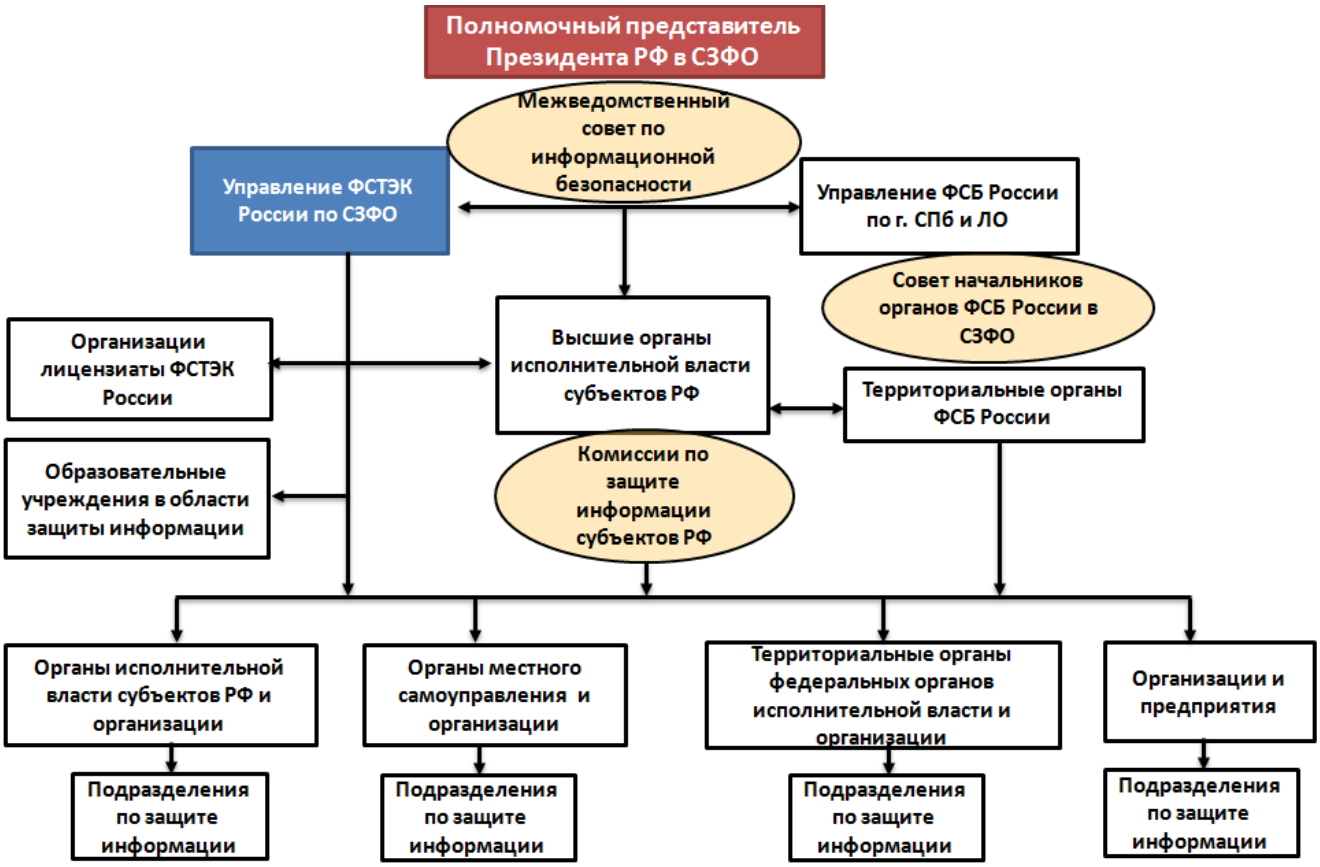


Рисунок 11. Структурная схема организации информационной безопасности в Северо-Западном федеральном округе

Первое и второе десятилетия XXI века для современного международного сообщества характеризуются развязыванием военных конфликтов между государствами и силового противостояния разных слоев общества внутри стран с применением не только вооруженных сил, но и современных информационно-коммуникационных технологий, социальной сети Интернет,, мгновенно распространяющей информацию о результатах любых событий через глобальное информационное пространство до всего мирового сообщества (примеры: Югославия – 1999 год; Ирак – 2003 год; Южная Осетия – 2008 год; Ливия – 2011 год; Сирия – 2011 год; Украина – 2014 год).

В «Стратегии национальной безопасности Российской Федерациидо 2020 года» отмечено, что возросла уязвимость всех членов международного сообщества перед лицом новых видов и угроз. Появились и угрозы информационной безопасности.

Анализ существующих и перспективных угроз информационной безопасности объектам округа за последнее время подтверждает, что эффективность иностранных технических разведок, возможности которых позволяют непрерывно вести слежение в отношении большинства объектов округа с целью добывания информации об экономике, научных разработках, новых технологиях, оборонном потенциале и других сведений, имеет тенденцию к возрастанию.

При этом легально, в соответствии с международными договорами и международными нормами, иностранными государствами на территории Северо-Западного федерального округа применяются:

- космические системы разведки;
- морские системы разведки в нейтральных водах и в территориальных водах России;
- воздушные системы разведки с полетами самолетов вдоль государственной границы;
- наземные системы разведки с территории иностранных государств (Норвегия – 8 постов, Финляндия – 10 постов, Эстония – 3 поста, Латвия – 3 поста, Литва – 2 поста станций радио- и радиотехнической разведки);
- наблюдательные полеты специально оборудованных самолетов, выполняемые в границах СЗФО в соответствии с Договором по открытому небу, позволяют детально «просмотреть» основные промышленные районы округа. При этом полеты в воздушном пространстве Калининградской области осуществляются фактически ежемесячно, что в первую очередь вызвано заявлением Верховного Главнокомандующего Российской Федерации о готовности развернуть ударные ракетные комплексы «Искандер» в ответ на развертывание системы ПРО в Европе;
- иностранные технические средства наблюдения и контроля, размещаемые и используемые на территории округа в ходе реализации международных научных, научно-технических программ и проектов;

− технические средства (стационарные, возимые, носимые), размещаемые в консульских учреждениях и международных организациях, аккредитованных при Министерстве иностранных дел.

Всего в пределах округа размещены 52 генеральных консульства и представительства иностранных государств, 32 из которых являются членами блока НАТО.

В качестве перспективных угроз информационной безопасности объектам СЗФО, по мнению автора, можно отнести следующие:

− использование современных информационных технологий и средств для осуществления враждебных действий и актов информационно-психологического воздействия против граждан, общественных структур и органов власти в регионе;

− целенаправленное деструктивное воздействие в информационном пространстве на критически важные структуры округа. Это, прежде всего, системы управления объектами энергетики (АЭС, ГЭС, ТЭЦ), транспорт (метро, морские порты, аэропорты), банковская сфера и др.;

− неправомерное использование информационных ресурсов объектов округа путем несанкционированного съема данных в своих интересах. Это в полной мере относится к информации персональных данных граждан, проживающих на территории СЗФО;

− использование регионального информационного пространства различного рода некоммерческими организациями, структурными группами и отдельными лицами в террористических, экстремистских и в иных преступных целях.

Всю совокупность данных факторов необходимо учитывать в практической деятельности по совершенствованию системы защиты информации в округе для снижения эффективности действий иностранных технических разведок и деструктивных структур.

Ранее автор, при рассмотрении главы 2, подробно останавливался на раскрытии содержания новых категорий: «информационный суверенитет» и «государственная политика информационного суверенитета», а также на

определении основных направлений их практической реализации как неотъемлемой части государственного суверенитета и национальной безопасности Российской Федерации в глобальном мире.

Для регионального уровня понятие информационного суверенитета можно сформулировать как верховенство и независимость государственной власти при формировании и реализации информационной политики в региональном сегменте Единого национального информационного пространства. Принципиальное значение для обеспечения информационного суверенитета в федеральном округе имеет государственная региональная информационная политика. Данная политика в СЗФО реализуется в информационно-технологической, информационно-психологической и в информационно-политической сферах.

Информационный суверенитет на региональном уровне предполагает наличие:

– в информационно-технологической сфере («цифровой» суверенитет) – собственного технологического цикла по производству информационно-коммуникационных средств, регионального компонента единой государственной поисковой и навигационной систем, сетевого оборудования и средств защиты информации отечественного производства, регионального сегмента сети Интернет и социальных сетей, части национальной платежной системы и др.

В данной связи следует привести мнение Вице-премьера правительства РФ Д. О. Рогозина: «Уверен, что в течение двух-трех лет мы будем готовы полностью избавиться от зависимости по комплектующим изделиям элементной базы, импортируемыми отечественными предприятиями ОПК из-за рубежа»[353];

– в информационно-психологической сфере *(«ментальный» суверенитет*) – адаптированных на региональный уровень государственных основ национальной идеи, высокого уровня информационной культуры и образованности общества, единого языка общения, религиозной, национальной толерантности и др.;

[353] Рогозин Д. О. Свой чип карман не тянет // Российская газета. 2014. 15 августа. № 184 (6456). С. 5.

– в информационно-политической сфере *(«властный» суверенитет*) – внятной региональной информационной политики, органов власти народного доверия и патриотически настроенной элиты регионального уровня, региональных средств массовой информации, выражающих региональные и государственные интересы.

Государственная политика информационного суверенитета на региональном уровне представляет собой деятельность государства и других органов исполнительной власти субъектов Российской Федерации по осуществлению самостоятельной информационной политики на основе существующих законов страны и норм международного права в информационной сфере с целью обеспечения верховенства информационной безопасности личности и всех структур общества в регионе.

Автор диссертации полагает, что государственная политика информационного суверенитета на региональном уровне должна реализовываться по следующим основным направлениям:

1. Определение и защита геополитических информационных интересов страны, региона в условиях глобализации всех основных сфер деятельности человечества (экономика, политика, идеология, дипломатия, вооруженные силы, культура, образование и др.).

2. Образование национальных и региональных (государственных и социальных) защищенных информационных сетей и систем, способных безопасно взаимодействовать с Глобальным информационным пространством.

3. Деятельность по созданию собственных сил и средств в области информационно-коммуникационных технологий.

4. Участие в международном сотрудничестве по реализации политики информационного суверенитета с руководством субъектов приграничных государств.

5. Участие в контроле информационных потоков как внутри региона, так и за его пределами с целью ограничения информации, пропагандирующей чуждые ценности.

С целью организации и координации деятельности всех элементов системы обеспечения информационной безопасности в СЗФО по противодействию техническим разведкам иностранных государств и технической защиты информации, по распоряжению полномочного представителя Президента Российской Федерации, в СЗФО в 2004 году создан Межведомственный совет по защите информации (далее – Совет).

Совет реализует государственную политику информационной безопасности применительно к региону путем осуществления своих полномочий во взаимодействии с территориальными органами федеральных органов власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления и с организациями ОПК, вузами. Совет рассматривает и утверждает ежегодные методические рекомендации в области информационной безопасности, которые являются обязательными к исполнению всеми вышеперечисленными структурами.

Итоги деятельности органов власти и подведомственных им организаций СЗФО по реализации государственной политики в области информационной безопасности Совет подводит в конце каждого года, основываясь на результатах контрольных проверок управлениями Федеральной службы безопасности и Федеральной службы по техническому и экспортному контролю.

При непосредственном участии автора были разработаны и доведены решениями Совета соответствующие политико-правовые, организационные и технические меры по противодействию добывания информации техническими средствами разведки.

Политико-правовые меры разрабатываются под руководством одного из высших должностных лиц субъекта Российской Федерации на основе действующих федеральных законов, нормативных документов федеральных служб-регуляторов в области информационной безопасности и рекомендаций Совета.

Организационные меры направлены на обеспечение всех элементов единой системы информационной безопасности региона основными нормативными и распорядительными документами и кадровой политики.

Технические меры, наряду с применением сертифицированных средств защиты информации, включают в себя диверсификацию доступа к коммуникационным средам и применение аппаратно-программных платформ с повышенной устойчивостью к деструктивным воздействиям.

Современные условия политического и социально-экономического развития России вызывают обострение противоречий между потребностями общества в развитии свободного обмена информацией и необходимостью сохранения отдельных регламентирующих ограничений на ее распространение.

В свою очередь, повышенное внимание технических разведок иностранных государств, криминальных структур к деятельности органов власти Северо-Западного федерального округа вызывает потребность в постоянном совершенствовании системы информационной безопасности.

В современном мире все более возрастают угрозы террористических действий, в том числе и со стороны кибертеррористов, в отношении информационных систем, управляющих критически важными объектами.

Интенсивное развитие информационных технологий, возрастание масштаба и опасности последствий нарушения требований безопасности информации для личности, общества и государства предполагает согласованные действия всех ветвей и уровней власти.

Все вышеперечисленные тенденции привели к пониманию необходимости дальнейшего развития системы информационной безопасности в округе с целью противодействия техническим разведкам по добыванию информации об объектах оборонно-промышленного комплекса, предприятиях энергетики, транспорта и недопущение деструктивного вмешательства в структуры технологического управления производством.

Для уточнения цели, задач, принципов организации основных направлений государственной политики информационной безопасности в части технической

защиты информации при участии автора была разработана и решением Совета введена в действие «Концепция защиты информации в Северо-Западном федеральном округе», представляющая собой цельную систему взглядов на проблему защиты информации, ее формирование и развитие.

Цель защиты информации в СЗФО определена «Концепцией…» как создание условий, способствующих реализации политики Российской Федерации в сфере обеспечения национальной безопасности, содействию устойчивому социально-экономическому развитию региона и государства в целом путем предотвращения (или существенного снижения) ущерба информационной безопасности в округе с использованием методов и средств защиты информации.

Для достижения поставленной цели потребуется решить целый ряд задач защиты информации в СЗФО.

В *экономической сфере* – обеспечение выгодных, с точки зрения защиты информации, условий для заключения международных экономических договоров, определения мест размещения организаций, предприятий, в том числе с участием иностранного капитала, а также предотвращение снижения эффективности экономической деятельности государственных организаций путем исключения (существенного затруднения) утечки информации или несанкционированного доступа к системам (средствам) информатизации и связи этих организаций со стороны иностранных государств, конкурентов или отдельных преступных лиц.

Во *внутриполитической сфере* – предотвращение несанкционированного доступа и специальных воздействий на контент в информационных системах и обеспечение безопасности данных в системах управления и электронного документооборота органов власти и других структур.

– обеспечение выгодных, с позиции национальной безопасности, условий по предотвращению ущерба от утечки информации о результатах фундаментальных и прикладных исследований, передовых технологиях и перспективных материалах, имеющих оборонное значение.

В «Концепции…» сформулированы основополагающие принципы защиты информации в СЗФО:

1) ***принцип системности и комплексности*** заключается в обеспечении безопасности информационных ресурсов, содержащих информацию с ограниченным доступом, в течение всего их жизненного цикла и при информационном взаимодействии с другими информационным системами (в частности, Интернетом); обеспечение надежной защиты информации от возможных угроз всеми доступными средствами и методами; способность системы к развитию и совершенствованию в соответствии с возможными изменениями условий ее функционирования;

2) ***принцип современности*** предусматривает постановку задач по комплексной защите информации, реализации мер по ее защите на ранних стадиях разработки информационных систем на основе анализа и прогнозирования, угроз информационной безопасности, а также разработку эффективных мер предупреждения посягательств на интересы государства в региональной информационной сфере;

3) ***принцип законности*** предполагает разработку системы защиты информации на основе федерального законодательства в области информатизации и защиты информации и других нормативных правовых актов по безопасности информации;

4) ***принцип научно-технической обоснованности*** состоит в использовании в регионе технических и программных средств, информационных технологий, средств защиты информации, реализованных на современном уровне развития науки и техники, научно и технически обоснованных с точки зрения достижения заданного уровня безопасности информации и его соответствия установленным нормам и требованиям;

5) ***принцип экономической целесообразности*** включает в себя достижение адекватного уровня затрат на обеспечение информационных ресурсов и величину возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать

экономические показатели работы органов власти и организаций, находящихся в пределах СЗФО;

6) ***принцип специализации и профессионализма*** нацелен на привлечение к разработке и внедрению мер и средств защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области;

7) ***принцип взаимодействия и координации*** заключается в выполнении комплекса мер по защите информации в соответствии с разработанными и согласованными планами совместных усилий заинтересованных органов власти и организаций;

8) ***принцип обязательности и эффективности контроля*** направлен на обязательность и своевременность выявления и пресечения попыток нарушения требований по безопасности информации в органах власти и в организациях;

9) ***принцип преемственности и непрерывности совершенствования*** включает в себя постоянное совершенствование мер и средств защиты информации с учетом наработанного и консолидированного опыта на основе анализа функционирования и перспектив развития систем и средств защиты информации;

10) ***принцип эффективности управления*** ориентирован на создание нормативных показателей, критериев и оценок состояния технической защиты информации.

«Концепцией…» определены основные направления деятельности по защите информации в СЗФО. Это организационно-режимное обеспечение защиты информации, которое включает обеспечение физической защиты объектов и средств информатизации; обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче на объектах информатизации; организацию защиты информации от несанкционированного доступа в автоматизированных информационных системах и локальных

вычислительных сетях; гарантирование конфиденциальности и целостности информации в средствах (системах) телекоммуникации и связи; достижение безопасного информационного взаимодействия с отечественными и зарубежными организациями; создание защиты информационных ресурсов от вредоносных программ; обеспечение комплексного контроля состояния и организации системы защиты информации на объектах защиты СЗФО.

Следующее важное направление – совершенствование нормативно-методической базы обеспечения защиты информации и организационно-штатной структуры подразделений, отвечающих за обеспечение защиты информации, а также подготовка специалистов по защите информации в регионе.

Перспективным направлением является организация и координация научно-исследовательских и опытно-конструкторских работ в области защиты информации. Основоопределяющим направлением является создание региональной многоуровневой системы по направлениям подбора, подготовки и переподготовки кадров в области защиты информации.

В пределах округа функционируют объекты атомной, химической, нефтеперерабатывающей отраслей: такие, как Кольская и Ленинградская атомные электростанции, акционерных обществ «Акрон», «ЛУКойл», «Киришинефтеоргсинтез» и др. В каждом субъекте также работают объекты жизнеобеспечения (тепло-, газо-, водо-, электроснабжения), нарушение функционирования которых может привести к непоправимым последствиям.

В настоящих условиях повышается зависимость органов власти от надежности функционирования государственных информационных систем, которые обеспечивают информационное сопровождение всех их функций во всех областях деятельности: экономике, политике, социальной сфере, военном деле, экологии и других. При этом тенденция увеличения количества и масштаба таких систем, в свою очередь, повышает риск потери управления при их недостаточной защищенности. Возрастает роль руководства субъектов в деятельности по обеспечению безопасности информации.

Таким образом, в современных условиях решить проблему обеспечения безопасности в информационных системах органов власти всех уровней, предприятиях ОПК, объектах энергетики, транспорта, банковской сферы для снижения (или предотвращения) потенциального ущерба национальной безопасности Российской Федерации в СЗФО возможно путем проведения мероприятий по последовательному совершенствованию политики информационной безопасности в регионе[354].

Организация подготовки специалистов в области информационной безопасности в высших учебных заведениях Северо-Западного федерального округа направлена на обеспечение потребностей органов власти и организаций в специалистах по направлению «Информационная безопасность», поддержание их квалификации на уровне современных требований.

Создана система подготовки кадров, которая является элементом системы защиты информации в Северо-Западном федеральном округе. Указанная система включает в себя Межведомственный совет по защите информации, комитеты по науке и высшей школе, комитеты по образованию в субъектах Российской Федерации и учреждения дополнительного профессионального образования.

Необходимо отметить, что действующая в Северо-Западном федеральном округе система подготовки кадров в области информационной безопасности, в целом, обеспечивает первоочередные потребности органов власти и организаций в специалистах.

С учетом вышеизложенного автором сформулирован ряд вопросов, которые требуют первоочередного решения:

– действующий механизм подготовки специалистов в области информационной безопасности по их количеству и номенклатуре слабо связан с их реальной потребностью, не содержит в себе обязательств выпускников вузов, подготовленных за счет федерального бюджета;

---

[354] См.: Сведения о взаимодействии Управления ФСТЭК России по Северо-Западному федеральному округу с иными органами государственной власти, организациями // http://fstec.ru/deyatelnost-szfo/vzaimodejstvie-szfo. (дата обращения: 09.12.2013)

– образовательные учреждения высшего профессионального образования, реализующие программы по направлению «Информационная безопасность», недостаточно обеспечены высококвалифицированными педагогическими кадрами и специализированной учебно-лабораторной базой, из-за чего они не в полной мере отвечают целям и задачам современного образовательного процесса;

– требует совершенствования система дополнительного профессионального образования, особенно в части наличия технических средств обучения, содержания образовательных программ и квалификации преподавателей.

* * *

По результатам исследования, представленным в данной главе, целесообразно сделать следующие выводы.

Во-первых, за два десятилетия существования Содружества Независимых Государств на постсоветском пространстве было разработано и принято большое число нормативно-правовых актов в области информационной безопасности, однако для большинства данных документов характерно терминологическое многообразие и слабая определенность используемого понятийного аппарата. В этой связи необходима унификация нормативных документов.

В современных условиях такая работа может быть наиболее эффективно осуществлена в рамках ОДКБ. Прежде всего, следует обратить внимание на совершенствование базовых терминов и понятий, используемых в области обеспечения информационной безопасности. Автором предложены некоторые подходы с целью выработки единой законодательной базы, направленной на сближение законодательства государств – членов ОДКБ в информационно-политической сфере и основные задачи по их решению.

Во-вторых, информационная сфера все больше превращается в арену для международного, межрегионального и межгосударственного соперничества, острейшей конкуренции в бизнесе, противоправных действий различного рода

криминальных структур. Крайними формами разрешения возникающих при этом конфликтов является информационный терроризм и информационные войны.

Все это создает опасные угрозы национальным интересам стран ОДКБ в информационной сфере. В рамках ОДКБ сформулирована и претворяется в практическую деятельность государств единая информационная политика по урегулированию политических, экономических, социальных и военных отношений как внутри организации – для обеспечения национальной безопасности государств, так и в глобальном мире – для реализации мер по поддержанию региональной безопасности всех государств – членов ОДКБ.

В-третьих, важнейшим компонентом национальной, региональной и международной безопасности в настоящее время становится информационная безопасность. Информационные технологии стали одним из важнейших политико-экономических и военных ресурсов. Совместная деятельность стран, в рамках СНГ и ОДКБ, в сфере обеспечения информационной безопасности преследует своей целью более эффективную защиту их законных интересов в информационном пространстве.

В-четвертых, скоординированная информационная политика государств – членов ОДКБ – важное приоритетное направление противодействия современным вызовам и угрозам, объединение совместных усилий по созданию системы коллективной безопасности.

В настоящее время общей стратегической целью в формате ОДКБ является формирование многофункциональной системы коллективной безопасности на основе дальнейшего совершенствования и повышения эффективности деятельности организации. Важной составляющей данной стратегической цели является обеспечение информационной безопасности в контексте дальнейшего регионального развития организации.

В-пятых, совершенствование политики информационной безопасности в СЗФО обусловлено рядом особых факторов, присущих только данному региону:

– геостратегическое положение, которое заключается в наличии сухопутных и морских границ со странами блока НАТО, расположение обособленного

субъекта Российской Федерации (Калининградской области), не имеющего общих границ с другими регионами округа;

– наличие значительного числа совместных предприятий (в том числе со странами дальнего зарубежья), консульств, иностранных торговых представительств;

– использование в органах власти всех уровней, предприятий и организаций различных отраслей промышленности систем и программного обеспечения иностранного производства, не сертифицированных по требованиям информационной безопасности в соответствии с требованиями федеральных законов и нормативных документов Российской Федерации, что может привести к нарушению режима функционирования систем и непредсказуемому ущербу с возможными человеческими жертвами;

– устойчивый рост деятельности иностранных технических разведок в отношении большинства объектов округа с целью добывания информации по экономике, научным разработкам, новым технологиям и других сведений об оборонном потенциале.

В-шестых, совершенствование системы защиты информации на региональном уровне в СЗФО, в силу указанных выше факторов, необходимо решать с использованием научных подходов.

Для регионального уровня было сформулировано понятие «информационный суверенитет» как верховенство и независимость государственной власти при формировании и реализации информационной политики в региональном сегменте национального информационного пространства. Проводимая государственная информационная политика в СЗФО реализуется в информационно-политической сфере («властный» суверенитет); в информационно-психологической («ментальный» суверенитет) и в информационно-технической («цифровой» суверенитет).

Автором сформулированы основные направления по формированию государственной политики информационного суверенитета на региональном уровне: определение информационных интересов региона в условиях

глобализации информационного пространства; образование региональных защищенных сетей, которые могут взаимодействовать с глобальным информационным пространством; создание в регионе собственных сил в области ИКТ; участие в проведении дипломатической деятельности по обеспечению информационного суверенитета за рубежом; контроль информационных потоков в регионе.

В-седьмых, все вышеперечисленные научные понятия: «информационный суверенитет государства», «государственная политика информационного суверенитета» на региональном уровне были положены автором в основу разработки «Концепции защиты информации в СЗФО».

«Концепция…» определяет основы решения таких задач, как: формирование и совершенствование системы защиты информации в СЗФО; разработка комплексного подхода к обеспечению защиты информации; подготовка и реализация предложений по совершенствованию политико-правового, научно-технического и организационного обеспечения защиты информации на объектах округа; определение основных направлений деятельности по защите информации всеми структурными элементами системы информационной безопасности в округе.

ЗАКЛЮЧЕНИЕ

Ситуация, сложившаяся в современном мире под влиянием процессов глобализации, геополитических трансформаций и становления информационного общества, во многом определяет для России новые требования по поддержанию национальной безопасности страны в условиях вновь возникающих угроз, исходящих из Глобального информационного пространства, что требует принятия соответствующих мер комплексной защиты.

Одним из основных действий по обеспечению национальной безопасности в инфосфере является своевременная реакция государства на обостряющееся информационное противоборство в мировом масштабе.

В связи с этим повышаются требования к системе обеспечения информационной безопасности России, а именно: к развитию сил и средств, используемых для информационного противоборства, а также к совершенствованию концептуальных и научных положений в предметной области.

Информационная безопасность – принципиально новый феномен в процессе защиты национальной безопасности России, сформировавшийся в течение нескольких прошедших десятилетий и ставший особо значимым в последнее время.

Изучение основных положений политической науки по вопросам обеспечения информационной безопасности государства показывает, что в наши дни идет процесс их формирования. В ходе этого процесса необходимо, прежде всего, учитывать следующие обстоятельства.

Во-первых, их формирование и развитие происходит, в целом, медленнее, чем развитие и изменение геополитических условий и связанных с ними угроз, исходящих из информационного пространства.

Во-вторых, имеющийся военно-политический, военно-научный и военно-технологический потенциалы в области обеспечения национальной безопасности

Российской Федерации предоставляют возможность создания высокоэффективной системы защиты информационного пространства на долгосрочную перспективу.

Для создания этой системы, как показывает проведенное исследование, необходимо решить следующие актуальные задачи:

1. Обеспечить инновационное и динамичное развитие информационно-коммуникационных технологий, способных учитывать и противодействовать не только существующим, но и перспективным угрозам информационной безопасности.

В условиях ограниченных временных и экономических ресурсов такая система должна быть ориентирована на парирование угроз и опасностей, имеющих, прежде всего, геополитический характер и направленных против жизненно важных сфер, процессов функционирования российского общества и государства.

2. Снизить эффективность разведывательной и иной деструктивной деятельности иностранных государств в национальном информационном пространстве, для чего проводить более активную государственную политику информационного суверенитета по защите национальных интересов в информационно-политической, информационно-психологической и в информационно-технологической сферах.

3. Создать, интенсивно развивать и поддерживать на должном военно-политическом уровне специальные силы и средства информационного противоборства, способные предотвращать возможный ущерб национальной безопасности государства в сложной современной геополитической обстановке.

4. Осуществлять постоянный и своевременный мониторинг состояния всей совокупности актуальных информационных угроз в контексте складывающейся мировой политической ситуации с целью качественного обеспечения информационной безопасности. Включить обобщенные выводы из данного мониторинга в «Стратегический прогноз Российской Федерации – документ

стратегического планирования, содержащий систему научно обоснованных представлений о стратегических рисках социально-экономического развития и об угрозах национальной безопасности Российской Федерации»[355].

Решение указанных задач предполагает реализацию соответствующих политических, экономических, военно-технических, дипломатических, международно-правовых и других мер, а также соответствующего теоретического обеспечения, в том числе и с позиций политологии. В данной связи наиболее перспективными направлениями дальнейших исследований являются:

1. Изучение взаимодействия традиционного геополитического пространства и быстро формирующегося и развивающегося глобального информационного пространства. Данные пространства взаимно влияют и дополняют одно другое. Возникают новые взаимосвязи между протекающими в них геополитическими и информационными процессами как на континентальном, так и на планетарном уровнях.

   Подобный анализ позволяет отслеживать изменения во взаимозависимости государств и регионов мира, в корректировке статусов стран в международном сообществе, в перемене положения сложившихся и возникновении новых центров силы и зон высокого развития мирового и регионального масштаба.

   Такого рода исследования имеют принципиальное значение для формирования и реализации государственной политики национальной безопасности Российской Федерации в условиях грядущего миропорядка.

2. Постоянный анализ основных тенденций глобального информационного пространства в контексте его дальнейшей политизации. Выявление новых форм политического воздействия с использованием информационного пространства на

[355] Федеральный закон от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании Российской Федерации». Ст. 3.

жизнедеятельность страны, осуществляемых из-за рубежа и непосредственно затрагивающих национальную безопасность России.

Политологическое исследование наиболее вероятных в будущем направлений информационного противоборства с позиции политической науки: прогнозирование геополитических целей, инновационных форм и способов ведения борьбы; определение наиболее перспективных национальных интересов в информационной сфере, имеющих политическую природу для их дальнейшего продвижения. Определение наиболее вероятных результатов влияния глобального противоборства на систему национальной безопасности страны с целью их учета при планировании мер по модернизации этой системы.

3. Исследование процесса военно-политической глобализации в контексте развития мирового информационного пространства с целью определения адекватных политических решений, направленных на повышение эффективности действий по защите национальной безопасности страны в условиях будущих информационных войн и вооруженных конфликтов.

4. Дальнейшее развитие современного понятийного аппарата политической науки в области изучения информационных аспектов национальной безопасности. Адаптация его к перспективным исследованиям в сфере информационного измерения политики национальной безопасности. Совершенствование системы категорий, позволяющих глубоко анализировать процессы и явления, имеющие место при сочетании информационной и политической составляющих национальной безопасности.

Центральное место в этой системе должны занимать категории «государственный информационный суверенитет» и «политика государственного информационного суверенитета».

5. Развитие методик квалиметрических оценок возможного ущерба государству в информационном пространстве. Продолжение научных разработок по их внедрению в исследование эффективности системы национальной безопасности Российской Федерации.

6. Изучение основных направлений и особенностей формирования культуры информационной безопасности в современной России. Раскрытие политических аспектов данной культуры, проведение анализа по ее влиянию на состояние национальной безопасности страны.

7. Комплексная работа по совершенствованию теоретических основ национальной политики компенсации и преодоления асимметрии в информационной сфере в отношениях России с США и НАТО.

8. Всестороннее исследование специфики процесса формирования общего информационного пространства государств – членов ОДКБ. Разработка рекомендаций по сближению и гармонизации законодательства стран организации с учетом новейших трансформаций геополитической картины мира и изменений в глобальном и региональном информационных пространствах.

9. Дальнейшая деятельность по внедрению «Концепции политики информационной безопасности в Северо-Западном федеральном округе» на период после 2015 года в среднесрочной перспективе, научное осмысление ее результатов и формирование основ теоретических исследований этой политики в региональных пространствах России.

Приложение

МЕТОДИКИ КВАЛИМЕТРИЧЕСКИХ ОЦЕНОК В ПОЛИТИЧЕСКИХ НАУКАХ

Введение

Количественные оценки, необходимые для анализа процессов, изучаемых в политических науках можно получить применением ряда методов и методик.

Из их числа можно выделить использование алгебраических, вероятностных и дифференциальных моделей, на которых «проигрываются» ситуации, а из полученных результатов в рамках заданного критерия качества формируются необходимые оценки.

К ним примыкают соответствующие игровые модели (антагонистические, коалиционные, иерархические, кооперативные).

Степень достоверности указанных выше моделей зависит от их сложности, качества реализации средствами вычислительной техники, сложности исследуемых процессов и явлений.

К недостаткам можно отнести трудоемкость получения экспресс-оценок, часто необходимых для практики.

В этих случаях можно применять оценки, основанные на построении квалиметрических шкал качества (систем, объектов и т.д.) в рамках заданного показателя качества, регрессионного анализа и др. Отметим, что сферы их применения к настоящему времени еще не исследованы.

Рассмотрим методики их получения.

1. Методика регрессионного анализа ущерба

В общем случае поставим задачу следующим образом.

Пусть имеется *i* случаев проявления результирующего параметра системы (в том числе: оценки тяжести ситуации, экономический ущерб государству и т.п.) U_i ($i = 1, 2, ..., m$). Сумма каждого конкретного значения параметра определяется ***de facto*** или оценивается экспертами. Результирующий параметр вызывается набором ряда факторов (причин) и характеризуется вектором исходных характеристик $\mathbf{x}_i = (x_{i1}, ..., x_{in}), \quad i = 1, ..., m, \quad n < m$. Введем вектор-функции $\varphi_j(\mathbf{x}_i) = (\varphi_j(\mathbf{x}_i), ..., \varphi_n(\mathbf{x}_i)), \quad n < m$ и вектор весовых коэффициентов $\mathbf{c} = (c_1, ..., c_n)$.

Представим «модельное» значение выходного параметра U по этим вектор-функциям в виде:

$$U = \sum_{j=1}^{n} c_j \varphi_j(x) \qquad (1)$$

Функции $\varphi_j(\mathbf{x}_i) = (\varphi_1(\mathbf{x}_i), ..., \varphi_n(\mathbf{x}_i)), \quad n < m$ задаются, а коэффициенты $c_1, ..., c_n$ можно определить из условия минимизации по ним суммы квадрата невязок $R^2 = \sum_{i=1}^{m} (U - U_i)^2$.

Из ряда вариантов возможных вариантов выбора функций $\varphi_j(\mathbf{x}_i) = (\varphi_j(\mathbf{x}_i), ..., \varphi_n(\mathbf{x}_i)), \quad n < m$ выбираем тот, который обеспечивает минимум суммы квадратов невязок.

В итоге из минимизации суммы квадратов невязок получаем следующую систему уравнений для нахождения коэффициентов $c_1, ..., c_n$ [1]:

$$\sum_{j=1}^{n} \left(\sum_{i=1}^{m} \varphi_j(x_i) \varphi_k(x_i) \right) c_j = \sum_{i=1}^{m} \varphi_k(x_i) U_i \qquad (2)$$
$$k = 1, ..., n$$

Для упрощения можно принять в качестве φ_j характеристику x_j, т.е.:

$$\sum_{j=1}^{n}\left(\sum_{i=1}^{m} x_{ij}\, x_{ik}\right) c_j = \sum_{i=1}^{m} x_{ik}\, U_i \qquad (3)$$
$$k = 1, \ldots, n$$

В качестве исходных характеристик можно применять длительность воздействия, степени информационного воздействия, степени секретности, вероятности защиты сведений, степени ущерба при нарушении режима секретности, уровни ущерба и т.п.

Для получения надежного результата системы линейных уравнений (2) или (3) лучше решать, используя сингулярное разложение [1]. Отметим, что вектор исходных характеристик допускает применение в качестве компонент и качественные характеристики «нет» и «да», обозначая их, соответственно, 0 и 1, а также «нет», «может быть», «да» (0, 0,5, 1).

Если коэффициенты $\mathbf{c} = (c_1, \ldots, c_n)$. найдены, то, используя формулу (1), находим оценки выходного параметра.

Методика позволяет при найденных коэффициентах определять комплексные оценки без привлечения экспертов.

Отметим, что моделей вида (1) может быть несколько. Лучшая их них та, которая обеспечивает минимум суммы квадрата невязок.

Отсюда получаем следующую методику использования регрессионного анализа.

Исходные данные: известные оценки выходного параметра (m случаев) в зависимости от компонент вектора исходных характеристик $\mathbf{x}_i = (x_{i1}, \ldots, x_{in}), \quad i = 1, \ldots, m, \quad n < m$.

1. Составляем функции $\varphi_j(\mathbf{x}_i) = (\varphi_j(\mathbf{x}_i), \ldots, \varphi_n(\mathbf{x}_i)), \quad n < m$ или принимаем вместо них $\varphi_j(\mathbf{x}_i) = x_{ij}$.
2. Решая системы уравнений (2) или, соответственно, (3), находим коэффициенты $\mathbf{c} = (c_1, \ldots, c_n)$.
3. Для заданного случая, используя формулу (1), определяем оценку

выходного параметра.

Рассмотрим в качестве иллюстрирующего примера №1 задачу квалиметрии конфликтов в международных делах с использованием регрессионного анализа. Исходные данные взяты из сайта «Всемирная история – Хронология новейшей истории 1945-2010. – http//infotables.ru/istoria. (Обр.: 09.07.2014)» и приведены в таблице …...

Таблица .

Международные конфликты 1945-2013 гг.

№ п/п	Название международного конфликта	Дата начала	Продол-житель-ность, лет	Вид	Использо-вание Вооружен ных Сил	Информа-ционное противо-борство	Сте-пень тяжести
1.	Гражданская война в Китае	1945	4	2	3	1	2
2.	Война за независимость Индокитая	1945	10	3	4	1	2
3.	Гражданская война в Греции	03.1946	3.6	2	3	0	1
4.	Индо-пакистанская война из-за Кашмира	08.1947	2.5	3	4	0	1
5.	Арабо-израильская война	05.1948	0.7	4	4	1	2
6.	Блокада Западного Берлина	06.1948	0.9	4	1	1	2
7.	Раскол Германии. Образование ГДР и ФРГ	05.1949	0.4	2	0	1	2
8.	Корейская война	06.1950	1.4	4	4	3	3
9.	Антисоветское восстание в Берлине	05.1953	0.05	1	1	1	1
10.	Суэцкий кризис. Ввод англо-французских войск. Захват Синайского полуострова	07.1956	0.67	4	4	1	3
11.	Венгерский кризис	10.1956	0.2	2	2	2	3
12.	Мятеж в Алжире. Независимость Алжира и других французских колоний	05.1958	3.9	1	2	0	1
13.	Гражданская война на Кубе	1957	2	1	2	0	1
14.	Провозглашение независимости республики Кипр	08.1960	2	1	0	0	1
15.	Берлинский кризис. Сооружение берлинской стены	08.1961	0.1	2	0	1	1
16.	Карибский кризис	10.1962	0.2	5	5	3	4
17.	«Белая» революция в Иране	01.1963	0.9	1	0	0	1
18.	Вьетнамская война	08.1964	10.4	3	4	2	3
19.	«Культурная» революция в Китае	05.1966	1	1	0	1	1
20.	Военный переворот в Греции	04.1967	0.1	1	1	0	1
21.	«Шестидневная» война арабских государств с Израилем	06.1967	0.02	4	4	2	3
22.	«Пражская» весна	03.1968	0.42	1	1	1	2
23.	Советско-китайский конфликт	03.1969	0.2	3	4	1	2
24.	Индо-пакистанская война	12.1971	0.042	3	4	1	3
25.	Арабо-израильская война	10.1973	0.058	4	4	2	3
26.	«Нефтяной» кризис	10.1973	0.2	4	0	1	2
27.	Кризис в Греции	11.1973	1.08	1	0	0	1
28.	Революция в Португалии	04.1974	0.1	1	0	0	0
29.	Кипрский кризис. Ввод турецких	07.1974	0.58	2	1	0	1

	войск						
30.	Революция «красных кхмеров»	1975	4	1	2	0	1
31.	Китайско-вьетнамская война	01.1979	0.2	3	4	1	2
32.	Исламская революция в Иране	02.1979	0.1	1	0	0	1
33.	Афганская война	12.1979	4	4	4	2	2
34.	Ливанская война	06.1982	0.2	3	4	2	2
35.	Оккупация Ираком территории Кувейта, вмешательство войск ООН во главе с США, разгром иракской армии (операция «Буря в Пустыне», 24-28.2.1991), освобождение Кувейта	08.1990	0,5	4	4	2	2
36.	Конфликт в Югославии: межэтническая война в Югославии и агрессия НАТО против Союзной Республики Югославия	1991-1995; 02.1998-1999	1,5	2	4	2	2
37.	Вторжение войск США и их союзников в Афганистан	10.2001	13	2	2	1	2
38.	Начало вторжения в Ирак войск США, Великобритании и их союзников	03.2003	8,4	4	4	3	2
39.	Вторжение израильской армии на территорию Ливана с целью покарать шиитскую группировку «Хезболла», завершившееся разрушением гражданской инфраструктуры Южного Ливана (большинство израильских войск выведено к 1.10.2006)	07.2006	0,1	2	2	2	2
40.	Вооружённый конфликт в Южной Осетии.	08.2008	0,04	2	2	3	2
41.	Война в Ливии	03.2011	0,75	4	2	3	2
42.	Операция по смене власти в Египте и Тунисе — «Арабская Весна»	2012	0,1	1	0	1	1
43.	Гражданская война в Сирии	2013	3,6	1	3	1	1

В качестве исходных параметров примем:

1) продолжительность конфликта

2) вид конфликта со следующими параметрами:

нет 0

внутренний 1

внутренний с вовлечением других стран 2

двухсторонний региональный 3

многосторонний региональный с числом государств 3-7 4

глобальный 5

3) степень использования Вооруженных Сил с параметрами:

нет 0

как средство военного, политического

и психологического давления	1
полицейская акция	2
гражданская война	3
региональная война	4

4) степень информационного противоборства с параметрами:

нет	0
слабая	1
средняя	2
тяжелая	3

Рассмотрим степень тяжести конфликта (по влиянию на международные отношения) с параметрами:

нет	0
слабая	1
средняя	2
тяжелая	3
катастрофическая	4

Построим регрессионную модель степени тяжести конфликта, разложив ее по продолжительности, виду, степени использования Вооруженных Сил, степени информационного противоборства в виде:

$$U = c_1 T + c_2 X + c_3 Y + c_4 Z \qquad (4),$$

где T - продолжительность конфликта; X - вид; Y - степень использования вооруженных сил, Z - степень информационного противоборства.

Решая систему линейных уравнений (3) методом сингулярного разложения матриц, получим следующие значения коэффициентов: $c_1 = 0.00882$, $c_2 = 0.41729$, $c_3 = 0.11564$, $c_4 = 0.34764$.

При этом сумма квадратов невязок составляет 11,5643, а среднеквадратичное отклонение невязок 0,52475.

Если домножить значения коэффициентов на оценки математических ожиданий соответствующих параметров, то получим абсолютные оценки

значений вклада в результат каждого из параметров: 0,0173, 1,0093, 0,2662, 0,4042 и относительные (отнесенные к значению математического ожидания степени тяжести конфликта) в процентах: 0,9536%, 55,6388%, 14,6770%, 22,2845%. Первое значение говорит о том, что степень тяжести конфликта в международных делах фактически мало зависит от его продолжительности, а на оценки степени тяжести больше влияет вид конфликта, и степень информационного противоборства, чем использование вооруженных сил.

Домножим коэффициенты на конкретные значения параметров из таблицы …. Результаты вычислений «выравненной» степени тяжести конфликта по математической модели (1) приведены в таблице ….

Таблица .

Международные конфликты 1945-2013 гг.

№ п/п	Название международного конфликта	Степень тяжести	Расчетное значение степени тяжести
1	Гражданская война в Китае	2	1,5644
2	Война за независимость Индокитая	2	2,1503
3	Гражданская война в Греции	1	1,2133
4.	Индо-пакистанская война из-за Кашмира	1	1,7365
5.	Арабо-израильская война	2	2,24855
6.	Блокада Западного Берлина	2	2,1404
7.	Раскол Германии. Образование ГДР и ФРГ	2	1,1857
8.	Корейская война	3	3,1870
9.	Антисоветское восстание в Берлине	1	0,8810
10	Суэцкий кризис. Ввод англо-французских войск. Захват Синайского полуострова	3	2,8329
11	Венгерский кризис	3	1,7629
12	Мятеж в Алжире. Независимость Алжира и других французских колоний	1	0,6830
13	Гражданская война на Кубе	1	0,6662
14	Провозглашение независимости республики Кипр	1	0,4349
15	Берлинский кризис. Сооружение берлинской	1	1,1831

	стены		
16	Карибский кризис	4	3,709
17	«Белая» революция в Иране	1	0,4252
18	Вьетнамская война	3	2,5014
19	«Культурная» революция в Китае	1	0,7738
20	Военный переворот в Греции	1	0,5338
21	«Шестидневная» война арабских государств с Израилем	3	2,8272
22	«Пражская» весна	2	0,8842
23	Советско-китайский конфликт	2	2,0624
24	Индо-пакистанская война	3	2,8275
25	Арабо-израильская война	3	2,06242
26	«Нефтяной» кризис	2	2,0186
27	Кризис в Греции	1	0,4268
28	Революция в Португалии	0	0,4182
29	Кипрский кризис. Ввод турецких войск	1	0,9553
30	Революция «красных кхмеров»	1	0,6859
31	Китайско-вьетнамская война	2	2,0638
32	Исламская революция в Иране	1	0,4182
33	Афганская война	2	2,0623
34	Ливанская война	2	2,0638
35	Оккупация Ираком территории Кувейта, вмешательство войск ООН во главе с США, разгром иракской армии (операция «Буря в Пустыне», 24-28.2.1991), освобождение Кувейта	2	2,8314
36	Конфликт в Югославии: межэтническая война в Югославии и агрессия НАТО против Союзной Республики Югославия	2	2,0056
37	Вторжение войск США и их союзников в Афганистан	2	1,5282
38	Начало вторжения в Ирак войск США, Великобритании и их союзников	2	3,2496
39	Вторжение израильской армии на территорию Ливана с целью покарать шиитскую группировку «Хезболла», завершившееся разрушением гражданской инфраструктуры Южного Ливана (большинство израильских войск выведено к 1.10.2006)	2	1,7620
40	Вооружённый конфликт в Южной Осетии.	2	2,950
41	Война в Ливии	2	2,1091

42	Операция по смене власти в Египте и Тунисе — «Арабская Весна»	1	0,7658
43	Гражданская война в Сирии	1	1,1436

Если принять за оценку уровня «информационного шума» оценку среднеквадратичного отклонения, то можно сделать вывод о том, что полученные экспертные значения степени тяжести конфликта в целом совпадают с расчетными. Отклонения вызваны как недостаточно обоснованными экспертными значениями степени тяжести конфликта, так и недостаточной полнотой модели вида (4).

Используем вычисленные значения коэффициентов для оценки степени тяжести конфликта на Украине (продолжительность конфликта – 0,5 лет, вид конфликта внутренний, полицейская акция использования Вооруженных сил, средний уровень информационного противоборства). Получим следующее значение: 1,4639(+-)0,5248. Таким образом, степень тяжести конфликта на Украине, вычисленная по модели (4), близка к средней.

Рассмотрим близкую к задаче №1 квалиметрии конфликтов – задачу №2. В ней будем использовать линейную свертку вида (5):

$$U = c_1 T + c_2 X + c_3 Y + c_4 Z + c_5 \qquad (5),$$

т.е. примем $\varphi_5(x) = 1$. Тогда коэффициент c_5 будет интегрально характеризовать неучтенные в предыдущей модели параметры.

Для нахождения коэффициентов составим уравнения вида (3) и решим их, используя метод сингулярного разложения матриц и те же самые исходные данные из таблицы ….. .

Получим следующие значения коэффициентов: $c_1 = -0.01460$, $c_2 = 0.22098$, $c_3 = 0.12200$, $c_4 = 0.36591$, $c_5 = 0.60174$.

При этом сумма квадратов невязок составляет 8,5398, а среднеквадратичное отклонение невязок 0,45092.

Если домножить значения коэффициентов на оценки математических ожиданий соответствующих параметров, то получим абсолютные оценки

значений вклада в результат каждого из параметров: - 0,02862, 0,53447, 0,28088, 0,42548, 0,60174 и относительные (отнесенные к значению математического ожидания степени тяжести конфликта) в процентах: -1,57784%, 29,46465%, 15,48425%, 23,4560%, 33,17294%. Первое значение, как и в предыдущем случае, говорит о том, что степень тяжести конфликта в международных делах фактически мало зависит от его продолжительности, а на оценки степени тяжести больше влияет вид конфликта, и степень информационного противоборства, чем использование вооруженных сил.

Относительно большое значение фактора неучтенных параметров (33,1729%) говорит о том, что такие параметры, как вид конфликта, использование Вооруженных сил, степень информационного противоборства недостаточно полно описывают степень тяжести конфликта.

Домножим коэффициенты на конкретные значения параметров из таблицы …. Результаты вычислений «выравненной» степени тяжести конфликта по математической модели (1) приведены в таблице ….

Таблица .

Международные конфликты 1945-2013 гг.

№ п/п	Название международного конфликта	Степень тяжести	Расчетное значение степени тяжести
1	Гражданская война в Китае	2	1,7172
2	Война за независимость Индокитая	2	1,9726
3	Гражданская война в Греции	1	1,3572
4.	Индо-пакистанская война из-за Кашмира	1	1,7162
5.	Арабо-израильская война	2	2,3294
6.	Блокада Западного Берлина	2	1,9605
7.	Раскол Германии. Образование ГДР и ФРГ	2	1,4038
8.	Корейская война	3	3,0510
9.	Антисоветское восстание в Берлине	1	1,3099
10	Суэцкий кризис. Ввод англо-французских войск. Захват Синайского полуострова	3	2,6957
11	Венгерский кризис	3	2,0166

12	Мятеж в Алжире. Независимость Алжира и других французских колоний	1	1,0098
13	Гражданская война на Кубе	1	1,0375
14	Провозглашение независимости республики Кипр	1	0,7935
15	Берлинский кризис. Сооружение берлинской стены	1	1,4082
16	Карибский кризис	4	3,4115
17	«Белая» революция в Иране	1	0,8096
18	Вьетнамская война	3	2,3327
19	«Культурная» революция в Китае	1	1,1740
20	Военный переворот в Греции	1	0,9433
21	«Шестидневная» война арабских государств с Израилем	3	2,7052
22	«Пражская» весна	2	1,3045
23	Советско-китайский конфликт	2	2,1157
24	Индо-пакистанская война	3	2,1180
25	Арабо-израильская война	3	2,7047
26	«Нефтяной» кризис	2	1,8487
27	Кризис в Греции	1	0,8070
28	Революция в Португалии	0	0,8213
29	Кипрский кризис. Ввод турецких войск	1	1,1572
30	Революция «красных кхмеров»	1	1,00833
31	Китайско-вьетнамская война	2	2,1157
32	Исламская революция в Иране	1	0,8213
33	Афганская война	2	2,6471
34	Ливанская война	2	2,1157
35	Оккупация Ираком территории Кувейта, вмешательство войск ООН во главе с США, разгром иракской армии (операция «Буря в Пустыне», 24-28.2.1991), освобождение Кувейта	2	2,6982
36	Конфликт в Югославии: межэтническая война в Югославии и агрессия НАТО против Союзной Республики Югославия	2	2,2416
37	Вторжение войск США и их союзников в Афганистан	2	1,4639
38	Начало вторжения в Ирак войск США, Великобритании и их союзников	2	2,9473
39	Вторжение израильской армии на территорию Ливана с целью покарать	2	2,0181

	шиитскую группировку «Хезболла», завершившееся разрушением гражданской инфраструктуры Южного Ливана (большинство израильских войск выведено к 1.10.2006)		
40	Вооружённый конфликт в Южной Осетии.	2	2,3849
41	Война в Ливии	2	2,8165
42	Операция по смене власти в Египте и Тунисе — «Арабская Весна»	1	1,1872
43	Гражданская война в Сирии	1	1,5021

Если принять за оценку уровня «информационного шума» оценку среднеквадратичного отклонения, то можно сделать вывод о том, что полученные экспертные значения степени тяжести конфликта также в целом совпадают с расчетными. Отклонения вызваны как недостаточно обоснованными экспертными значениями степени тяжести конфликта, так и недостаточной полнотой модели вида (5).

Используем вычисленные значения коэффициентов для оценки степени тяжести конфликта на Украине (продолжительность конфликта – 0,5 лет, вид конфликта внутренний, полицейская акция использования Вооруженных сил, средний уровень информационного противоборства). Получим следующее значение: 1,9133 (+ –)0,4509. Таким образом, степень тяжести конфликта на Украине, вычисленная по модели (5), близка к средней.

2. Методика нахождения квалиметрических показателей на основе линейных сверток для комплексных количественных оценок в политических науках

Нахождение квалиметрических показателей (оценок) и построение на их основе квалиметрических шкал качества можно произвести на следующей методической основе.

В ряде случаев для комплексных оценок трудно выделить один показатель для проведения регрессионного анализа или в общем случае явление не имеет количественных измерений.

Тогда можно поступить следующим образом.

Пусть в описании явления (события) участвует n компонент вектора характеристик $x=(x_1,...,x_n)$. Если известны m проявлений вектора характеристик $x_i=(x_{i1},...,x_{in})$, то составим из них вектор-функции $\varphi_j(\mathbf{x}_i)=(\varphi_j(\mathbf{x}_i),...,\varphi_n(\mathbf{x}_i)), \quad n<m$.

В частном случае можно принять в качестве φ_j характеристику x_j.

Отметим, что вектор исходных характеристик допускает применение в качестве компонент и качественные характеристики «нет» и «да», обозначая их, соответственно, 0 и 1, а также «нет», «может быть», «да» (0, 0,5, 1).

Для количественных оценок явления (события) используем линейную свертку вида:

$$J=\sum_{j=1}^{n} c_j\varphi_j(x) \qquad (4)$$

Где $\mathbf{c}=(c_1,...,c_n)$ - вектор коэффициентов.

Коэффициенты $\mathbf{c}=(c_1,...,c_n)$ можно найти из экспертных оценок, что определяет соответствующую группу методов. К этой группе методов тесно примыкает метод индексов (индексный метод), отличающийся от предыдущего способом пересчета коэффициентов $\mathbf{c}=(c_1,...,c_n)$ (см., например, [2].

Линейная свертка допускает количественную оценку квалиметрического показателя и в том случае, когда исходная система является иерархической: компоненты вектора характеристик тогда в свою очередь являются значениями соответствующих сверток.

Недостатком такого подхода обычно является проблема экспертов: их поиска, достаточного количества и т.д. Поэтому разрабатывались и другие методы нахождения коэффициентов сверток путем обработки баз данных, в их

числе методы многоцелевой оптимизации, теории квалиметрических шкал качества Н.В. Хованова, метод условного показателя и др. [3–7].

В частности, Хововановым [4,5] доказано, что коэффициенты в линейных свертках определяются как вероятности проявления доминант в таблицах данных.

Как показано в работе [7] коэффициенты линейной свертки можно найти из решения систем линейных уравнений относительно некоторой вводимой для оцифровки события (явления) некоторой условной единицы J_0:

$$\sum_{j=1}^{n}\left(\sum_{i=1}^{m}\varphi_j(x_i)\,\varphi_j(x_i)\right)c_j = m\,J_0\,\varphi_{0k}(x),\quad k=1,\ldots,m, \qquad (5)$$

где $\varphi_{0k}(x_j)=\dfrac{\sum_{i=1}^{m}\varphi_k(x_i)}{m}$ — среднеарифметическое значение функций $\varphi_k(x_i)$.

Для получения надежного результата системы линейных уравнений (5) лучше решать, используя сингулярное разложение [1]. Отметим, что вектор исходных характеристик допускает применение в качестве компонент и качественные характеристики «нет» и «да», обозначая их, соответственно, 0 и 1, а также «нет», «может быть», «да» (0, 0,5, 1).

Домножая полученные коэффициенты на функции $\varphi_j(x_i)$, определим значение линейной свертки $J=\sum_{j=1}^{n}c_j\varphi_j(x)$.

Отсюда формируется следующая методика нахождения квалиметрических показателей на основе линейных сверток.

Исходные данные: m случаев проявления компонент вектора исходных характеристик $\mathbf{x}_i=(x_{i1},\ldots,x_{in}),\quad i=1,\ldots,m,\quad n<m$.

1) Составляем функции $\varphi_j(\mathbf{x}_i)=(\varphi_j(\mathbf{x}_i),\ldots,\varphi_n(\mathbf{x}_i)),\quad n<m$ или принимаем вместо них $\varphi_j(\mathbf{x}_i)=x_{ij}$.
2) Решая систему уравнений (5) или, соответственно, определяя вероятности проявление доминант, находим коэффициенты

$\mathbf{c} = (c_1,..., c_n)$.

3) Для заданного случая, используя формулу (4), определяем квалиметрический показатель качества явления (события).
4) Из набора квалиметрических показателей формируем квалиметрическую шкалу качества.

Пример. Имеются 11 систем, каждая из которых описывается определенным вектором состояний x_j. В качестве показателя сравнения примем линейную свертку вида $J_j = \sum_{i=1}^{4} c_i x_{ji}$. Таким образом, в рамках данного примера $\varphi_{ji} = x_{ji}$. Условное значение показателя сравнения J_0 примем равным единице. Требуется выбрать систему с максимальным значением J.

Исходные значения компонентов вектора состояния каждого изделия представлены в таблице 1.

Таблица 1.

Значения компонентов вектора состояния группы систем

Номер системы	x_{j1}	x_{j2}	x_{j3}	x_{j4}
1	131	0.02857	0.14286	0.1014
2	165	0.02157	0.15686	0.0823
3	127	0.03231	0.12308	0.0833
4	144	0.03537	0.15291	0.0833
5	112	0.03817	0.10753	0.0833
6	152	0.02473	0.14545	0.0833
7	129	0.03407	0.08889	0.1666
8	154	0.03030	0.16418	0.0833
9	146	0.02853	0.14139	0.0833
10	120	0.04132	0.13889	0.2600
11	120	0.03757	0.11834	0.0912

После проведения вычислений с использованием сингулярного разложения получены следующие значения весовых коэффициентов c_i, $i = 1,...,4$: $0.00524388,\ 12.81753887,\ -0.83767837,\ -0.13320216$. Используя их, найдем

условные показатели: $J_1 = 0.9200$, $J_2 = 0.9993$, $J_3 = 0.9659$, $J_4 = 1.0693$, $J_5 = 0.9754$, $J_6 = 0.9811$, $J_7 = 1.0166$, $J_8 = 1.0473$, $J_9 = 1.0018$, $J_{10} = 1.0079$, $J_{11} = 0.9996$.

Как видно из представленных результатов, четвертая система имеет наибольшее значение показателя сравнения $1{,}0693$.

ИСТОЧНИКИ И ЛИТЕРАТУРА

ИСТОЧНИКИ:

Нормативно-правовые акты и документы Российской Федерации:

1. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] / Утв. Президентом РФ от 9 сентября 2000 г. № Пр-1895. – Режим доступа: http:// www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr. html. (дата обращения: 27.09.2013)

2. Информационное общество (2011–2020 гг.): Государственная программа Российской Федерации / Утв. распоряжением Правительства Российской Федерации от 20 октября 2010 г. № 1815-р. – Гл 2. (дата обращения: 04.05.2013)

3. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве [Электронный ресурс] / Министерство обороны России, 2011 г. – Режим доступа: http://ens.mil.ru/science/ publications/more.htm?id=10845074@cmsArticle. (дата обращения: 05.09.2012)

4. О стратегическом планировании Российской Федерации: Федеральный закон от 28 июня 2014 г. № 172-ФЗ; Ст. 3.

5. Об информации, информатизации и о защите информации: Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ.

6. О государственной программе Российской Федерации «Информационное общество (2011-2020 гг.): Распоряжение Правительства РФ от 20.10.2010 № 1815-р (ред. от 15.08.2012).

7. Положение о межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности // Конституционно-правовой статус Совета Безопасности Российской Федерации / Под общ. ред. Н. П. Патрушева; 2-е изд., испр. и доп. – М.: Изд-во «Известия», 2013. – С. 263-266.

8. Положение о Федеральной службе по техническому и экспортному контролю [Электронный ресурс] / Утверждено Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (редакция от 21.12.2013). – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_156349/?fra me=1. (дата обращения: 10.02.2014)

9. Путин В. В. Послание Президента Федеральному Собранию [Электронный ресурс]. – 12 декабря 2012 г. – Режим доступа: http://президент.рф/news/17118. (дата обращения: 23.10.2013)

10. Стратегия национальной безопасности Российской Федерации до 2020 г. / Утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537 // Российская газета. – 2009. – 19 мая.

11. Стратегия развития информационного общества в Российской Федерации / Утверждена Президентом Российской Федерации В. В. Путиным 7 февраля 2008 г. № Пр-212 // Российская газета. – 2008. – 11 февраля.

12. Сведения о взаимодействии Управления ФСТЭК России по Северо-Западному федеральному округу с иными органами государственной власти, организациями [Электронный ресурс]. – Режим доступа: http://fstec.ru/deyatelnost-szfo/vzaimodejstvie-szfo. (дата обращения: 09.12.2013)

Нормативно-правовые акты и документы зарубежных государств:

13. Конституция Исламской Республики Иран [Электронный ресурс]. – Ашхабад: Культурный центр Посольства ИРИ в Туркменистане, 2007. – 319 с. – Режим доступа: http://worldconstitutions.ru/?p=83. (дата обращения: 25.10.2013)

14. Конституция Российской Федерации / Принята на всенародном голосовании 12 декабря 1993 г. (с поправками) [Электронный ресурс]. – Режим доступа: http://www.constitution.ru. (дата обращения: 10.07.2013)

15. Концепция внешней политики Российской Федерации [Электронный ресурс] / Утверждена Президентом Российской Федерации В. В. Путиным 12 февраля 2013 г. – Режим доступа: http://www.mid.ru/brp_4.nsf/0/6D84DDEDEDBF7DA644257B160051BF7F. (дата обращения: 18.03.2013)

16. О защите информации: Закон Республики Таджикистан от 02.12.2002 г. № 71.

17. О свободе информации: Закон Республики Армения от 23.09.2003 г. № 3Р-11.

18. О Совете национальной безопасности и обороны Украины: Закон Украины от 5 марта 1998 г. № 183/98-ВР. (дата обращения: 18.12.2013)

19. Об информатизации: Закон Кыргызской Республики от 08.10.1999 г. № 107.

20. Об информатизации: Закон Республики Казахстан от 11.01.2007 г. № 217-III.

21. Об информатизации: Закон Республики Таджикистан 06.08.2001 г. № 40.

22. Об информации, информатизации и защите информации: Закон Республики Беларусь от 10.11.2008 г. № 455-З.

23. Об информации: Закон Республики Таджикистан от 10.05.2002 г. №55

Международно-правовые акты и документы:

24. Глобальная программа кибербезопасности (ГПК) МСЭ. Основа для международного сотрудничества в области кибербезопасности [Электронный ресурс]. – Женева: МСЭ, 2008. – Режим доступа: http://www.ifap.ru/pr/2008/080908aa.pdf. (дата обращения: 07.02.2014)

25. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция Генеральной Ассамблеи ООН № A/RES/64/25 от 2 декабря 2009 года [Электронный ресурс]. – Режим доступа: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/463/35/PDF/N0946335.pdf?Open Element. (дата обращения: 19.02.2014)

26. Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности: Доклад Международного союза электросвязи [Электронный ресурс]. – Женева: МСЭ, 2010. – Режим доступа: http://www.itu.mt/ dms_pub/itu-d/opb/stg/D-STG-SG01.22-2010-PDF-R.pdf. (дата обращения: 19.02.2014)

27. Информационно-коммуникационные технологии, общеорганизационное планирование ресурсов и обеспечение безопасности,

послеаварийного восстановления и бесперебойного функционирования систем: Резолюция Генеральной Ассамблеи ООН № A/RES/63/262 от 24 декабря 2008 года [Электронный ресурс]. – Режим доступа: http://daccess-dds-ny.un.org/doc/UNDOC/ GEN/N08/486/53/PDF/N0848653.pdf?OpenElement. (дата обращения: 20.10.2013)

28. Использование информационно-коммуникационных технологий в целях развития: Резолюция Генеральной Ассамблеи ООН № A/RES/65/141 от 20 декабря 2010 года [Электронный ресурс]. – Режим доступа: http://daccess-dds-ny.un.org/ doc/UNDOC/GEN/N10/521/02/PDF/N1052102.pdf?OpenElement. (дата обращения: 19.02.2014)

29. Концепция Конвенции об обеспечении международной информационной безопасности [Электронный ресурс] / Разработана ИПИБ МГУ; представлена Россией 21-22 сентября 2011 года в Екатеринбурге на Второй Международной встрече высоких представителей, курирующих вопросы безопасности. – Режим доступа: http://www.aciso.ru/news/3255. (дата обращения: 18.10.2012)

30. Конвенция об обеспечении международной информационной безопасности: концепция [Электронный ресурс]. – Режим доступа: http://www.scrf.gov.ru/documents/6/112.html. (дата обращения: 18.01.2014)

31. Концепция сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности [Электронный ресурс] / Утверждена решением СГГ СНГ от 10 октября 2008 г. – Режим доступа: http://base.consultant.ru/cons/cgi/onJine.cgi?req=doc;base=INT;n=44Q89. (дата обращения: 12.01.2014)

32. Концепция формирования информационного пространства СНГ [Электронный ресурс] / Утверждено решением СГП СНГ от 18 октября 1996 г. – Режим доступа: http://www.zakonprost.ru/content/base/41929. (дата обращения: 17.02.2013)

33. Модельный информационный кодекс для государств – участников СНГ // Информационный бюллетень МПА СНГ. – 2013. – № 57. – Часть I. – С. 44-73.

34. О международном информационном обмене: Модельный закон МПА СНГ от 26.03.2002 г.

35. Об электронных государственных услугах: Модельный закон МПА СНГ от 7.04.2010 г.

36. Окинавская Хартия глобального информационного общества [Электронный ресурс]. – Окинава, 22 июля 2000 г. – Режим доступа: http://www.iis.ru/library/okinawa/charter.ru.html. (дата обращения: 19.11.2013)

37. Положение о разработке модельных законодательных актов и рекомендаций Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств: Постановление МПА СНГ от 23.11.2012 г. № 38-24.

38. Расширение доступа к Интернету благодаря трансъевразийской высокоскоростной информационной магистрали: Резолюция Генеральной Ассамблеи ООН № A/RES/64/186 от 21 декабря 2009 года [Электронный ресурс]. – Режим доступа: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/473/01/PDF/N0947301.pdf?OpenElement. (дата обращения: 15.02.2014)

39. Соглашение между Правительством Российской Федерации и Правительством Федеративной Республики Бразилии о сотрудничестве в области обеспечения международной информационной и коммуникационной безопасности (от 14 мая 2010 г.) // Международные правовые акты и документы в области международной информационной безопасности. – М., 2012. – С. 80-87.

40. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества в области обеспечения международной информационной безопасности от 16 июня 2009 года // Бюллетень международных договоров. – М.: 2012. – № 1. (дата обращения: 25.10.2013)

41. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20.11.2013 г.

42. Соглашение о сотрудничестве государств – членов Организации Договора о Коллективной Безопасности в сфере информационной безопасности

от 10.12.2010 г.

43. Communication from the Commission to the Council, the European parliament, the European Economic and Social Committee and the Committee of the Regions «Network and Information Security: Proposal for A European Policy Approach». Brussels, 6.6.2001. COM (2001) 298 final.

ЛИТЕРАТУРА:

Монографии:

1. Араб-Оглы, Э. А. Обозримое будущее. Социальные последствия НТР: год 2000 / Э. А. Араб-Оглы. – М.: Мысль, 1986. – 205 с.

2. Арбатов, А.Г. Разоружение и безопасность2001-2002: Международная безопасность: новые угрозы нового тысячелетия / А.Г. Арбатов.- Рос. Акад. Наук, Ин-т мировой эконом. И междунар. Отношений, Центр геополит. И военных прогнозов.- М.: Наука, 2003.- 395с.

3. Ачкасов, В. А. Модернизация России и Китая: проблемы теории и политическая практика: коллективная монография / Под ред. В. А. Ачкасова и С. А. Ланцова. – СПб.: Изд. С.-Петербургского университета, 2012. – 184 с.

4. Балуев, Д. Г. Информационно-коммуникационные измерения политических процессов / Д. Г. Балуев и др.; под общ. ред. академика О. А. Колобова. – Н.Новгород: ННГУ, 2006.– 107 с.

5. Безопасность на Западе и Востоке и в России: представления, концепции, ситуации: материалы международной научной конференции / Под ред. С. А. Панапина, Д. И. Полывянного. – Иваново: Ивановский гос. ун-т., 2013. – 408 с.

6. Белозёров, В. К. Стратегия национальной безопасности Российской Федерации до 2020 года: проблемы реализации: монография / В. К. Белозёров и др. – М.: Издательский дом «АТИСО», 2011.

7. Бестужев-Лада, И. В. Нормативное социальное прогнозирование.

Возможные пути реализации целей общества / И. Л. Бестужев-Лада. – М.: Наука, 1987. – 214 с.

8. Бестужев-Лада, И. В. Поисковое социальное прогнозирование: перспективные проблемы общества / И. Л. Бестужев-Лада. – М.: Наука, 1984. – 271 с.

9. Богатуров, А. Д. Россия в современной среде международной безопасности / А. Д. Богатуров // Россия в формировании международной системы профилактики распространения оружия массового поражения; отв. ред. А. А. Кокошин, А. Д. Богатуров. – М.: КомКнига, 2008. – С. 14-35.

10. Богомолов, В. А. Экономическая безопасность / В. А. Богомолов, Н. Д. Эриашвили.– М.: ЮНИТИ, 2010. – 228 с.

11. Боден Ж. Шесть книг о государстве //Антология мировой политической мысли: В 5 т. Т.2. М., 1999. С.689–695.

12. Борщ, А. А. Национальная безопасность и власть / А. А. Борщ. – М.: РАНХиГС при Президенте Российской Федерации, 2012. – 376 с.

13. Вилков, А. А. Политическая функциональность современных российских СМИ / А. А. Вилков, С. Ф. Некрасов, А. В. Россошанский. – Саратов: Изд-во «Научная книга», 2011. – 268 с.

14. Вишняков, Я. Д. Общая теория рисков / Я. Д. Вишняков, Н. Н. Радаев. – 2-е изд., испр. – М.: Издательский центр «Академия», 2008. – 368 с.

15. Возженников, А. В. Национальная безопасность России: методология комплексного исследования и политика обеспечения: монография / А. В. Возженников. – М.: Изд-во РАГС, 2002. – 423 с.

16. Воронцова, Л. В. История и современность информационного противоборства / Л. В. Воронцова, Д. Б. Фролов.– М.: Горячая линия – Телеком, 2006. – 192 с.

17. Вус, М.А. Информатика: Введение в информационную безопасность / М.А. Вус, В.С. Гусев, Д.В. Долгирев, А.А. Молдовян – СПб.: Изд-во «Юридический центр Пресс», 2004.-216 с.

18. Глобальная безопасность: инновационные методы анализа конфликтов

/ Под общ. ред. А. И. Смирнова. – М.: Общество «Знание» России, 2011. – 272 с.

19. Гоббс Т. Избранные произведения: в 2 т. М., 1964. Т. 1. 448 с.

20. Гончаренко, Л. П. Управление безопасностью / Л. П. Гончаренко, Е. С. Куценко. – М.: Изд-во «Кронус», 2010. – 272 с.

21. Друкер, П. Менеджмент. Вызовы XXI в. / П. Друкер. – М.: Изд-во «Манн, Иванов и Фербер», 2012. – 256 с.

22. Загладин, В. В. Глобальные проблемы современности: научный и социальный аспекты / В. В. Загладин, И. Т. Фролов. – М.: Международные отношения, 1981. – 240 с.

23. Загладин, Н.В. Стратегический глобальный прогноз, 2030: расширенный вариант / Н.В. Загладин.-Ин-т мировой экономики и междунар. Отношений РАН.- Мю:Магистр, 2011.-477с.

24. Законодательство государств - членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности: опыт, проблемы и перспективы гармонизации / Материалы Международной научно-практической конференции (Санкт-Петербург, 28.11.2013). – СПб: Секретариат Совета МПА СНГ, 2014. – 88 с.

25. Ивашов, Л. Г. Россия или Московия? Геополитическое измерение национальной безопасности России / Л. Г. Ивашов. – М.: Изд-во «Эксмо», 2002. – 416 с.

26. Инновационные направления современных международных отношений / Под ред. А. В. Крутских и А. В. Бирюкова. – М.: Аспект Пресс, 2010. – 295 с.

27. История международных отношений. В 3 тт. / Под ред. А. В. Торкунова, М. М. Наринского. – М.: Аспект Пресс, 2012. – Т. 1. – С. 193-194.

28. Кокошин, А. А. Политико-военные и военно-стратегические проблемы национальной безопасности России и международной безопасности / А. А. Кокошин. – М.: Высшая школа экономики, 2013. – 261 с.

29. Комов, С. А.Термины и определения в области информационной безопасности / С. А. Комов, В. В. Ракитин, С. Н. Родионов С. Н. [и др.]. –

М.: Издательство «АС-Траст», 2009. – 304 с.

30. Коровянский, А. И. Военная безопасность Российской Федерации и ее обеспечение в современных условиях / А. И. Коровянский. – М.: Изд-во РАГС, 2010. – 218 с.

31. Косов, Ю. В. Политическая регионалистика / Ю. В. Косов, В. В. Фокина. – СПб: Питер, 2009. – 192 с.

32. Кременюк, В. А. Россия и США в новых международных условиях: асимметричное партнерство? / В. А. Кременюк. – М.: Ин-т США и Канады РАН, 2005. – 91 с.

33. Кулагин, В. М. Международная безопасность / В. М. Кулагин. – М.: Аспект Пресс, 2007. – 258 с.

34. Кулагин, В.М. Современная международная безопасность / В.М. Кулагин.- М.: КноРус, 2012.- 431с.

35. Ланцов, С. А. Террор и террористы: словарь / С. А. Ланцов. – СПб.: Изд-во С.-Петербургского ун-та, 2004. – 187 с.

36. Маклюэн, М. Галактика Гутенберга. Становление человека печатающего / М. Маклюэн.– М.: Академический проект, 2005. – 496 с.

37. Маклюэн, М. Понимание медиа: внешние расширения человека / М. Маклюэн. – М.: Кучково поле, 2007. – 464 с.

38. Манойло, А. В. Государственная информационная политика в условиях информационно-психологической войны / А. В. Манойло, А. И. Петренко, Д. Б. Фролов. – М.: Горячая линия – Телеком, 2012. – С. 97-98.- 478 с.

39. Медиакратия: современные теории и практики / Под ред. А. С. Пую, С. С. Бодруновой. – СПб.: Изд-во С.-Петерб. ун-та, 2013. – 352 с.

40. Научные и методологические проблемы информационной безопасности (сборник статей). Под ред. В.П. Шерстюка. – М.: МЦНМО, 2004. – 208 с.

41. О глобализации, информатизации и национальной безопасности России: аналитический обзор / Под ред. С. А. Таразевича. – СПб: Телерос, 2010. – С. 26, 40-43, 83.

42. Осипов, В. И. Опасные природные процессы – стратегические риски

России / В. И. Осипов.– М.: РБОФ «Знание» им. С. И. Вавилова, 2009. – 40 с.

43. Панцерев, К. А. Страны тропической Африки в системе современных международных отношений / К. А. Панцерев. – СПб: Изд-во СПбГУ, 2011. – 212 с.

44. Пирумов, В. С. Информационное противоборство. Четвертое измерение противостояния / В. С. Пирумов. – М.: «Оружие и технологии», 2010. – 252 с.

45. Пую, А. С. Информационные технологии и терроризм: теория и современная практика / А. С. Пую, Н. С. Лабуш, А. Ю. Евсеев. – СПб.: Роза мира», 2005. – 147 с.

46. Радиков, И. В. Политика и национальная безопасность: монография / И. В. Радиков. – СПб.: Астерион, 2004. – 348 с.

47. Руссо Ж. Ж. Об общественном договоре. Трактаты / Пер. с фр. М.: КАНОН-пресс, Кучково поле, 1998. 416 с.

48. Смирнов, А.И. Информационная глобализация и Россия: вызовы и возможности / А.И. Смирнов.- М.: ПАРАД, 2005.- 391с.

49. Современная мировая политика: Прикладной анализ / Отв. ред. А. Д. Богатуров. – М.: Аспект Пресс, 2010. – 588 с.

50. Современные международные отношения и мировая политика / Отв. ред. А. В. Торкунов. – М.: Просвещение: МГИМО, 2004. – 991 с.

51. Стратегические риски России: оценка и прогноз / Под общ. ред. Ю. Л. Воробьева. – М.: Деловой экспресс, 2005. – 392 с.

52. Тоффлер, О. Третья волна / О. Тоффлер. – М.: Изд-во АСТ, 2010. – 784 с.

53. Уткин, А. И. Мировая холодная война / А. И. Уткин. – М.: Эксмо, Алгоритм, 2005. – 736 с.

54. Филимонов, Г. Ю. Культурно-информационные механизмы внешней политики США. Истоки и новая реальность / Г. Ю. Филимонов. – М.: РУДН, 2012. – 408 с.

55. Худолей, К. К. Россия в информационном поле зарубежных СМИ и

Интернет в 2011 г.: модели восприятия и механизмы их формирования / К. К. Худолей, Д. А. Болотов, Е. Ю. Трещенков, А. М. Седов, Д. И. Максимова. – СПб.: «Левша», 2012. – 59 с.

56. Худолей, К.К. Россия и европейская интеграция: прошлое, настоящее, будущее /К.К. Худолей.-Спб: Издательство СПБГУ, 2012.- 332с.

57. Цыганков, П.А. Универсальные ценности в мировой и внешней политике / П.А. Цыганков, Г.А.Дробот, В.А. Гуторов и др.; Под ред.П.А. Цыганкова. — М.: Издательство Московского университета, 2012. — 224 с.

58. Чернов, А. А. Становление глобального информационного общества: проблемы и перспективы / А. А. Чернов. – М.: «Дашков и К°», 2003. – 232 с.

59. Шакин, Д. Н. Информационная безопасность: коллективная монография / Д. Н. Шакин (руководитель), Е. Г. Бунев, С. М. Доценко, В. С. Пирумов, С. И. Тынянкин и др. – М.: Оружие и технологии, 2009. – 264 с.

60. Шестопал, Е. Б. Образы государств, наций и лидеров / Е. Б. Шестопал. – М.: Аспект Пресс, 2008. – 288 с.

61. Шмитт Карл. Политическая теология. М.: Канон-пресс-Ц, 2000. С. 7-98.

62. Шульц, В. Л. Диагностика и сценарный анализ угроз социально-экономическому развитию Арктической зоны Российской Федерации / В. Л. Шульц, В. В. Кульба, А. Б. Шелков, И. В. Чернов. – М.: РАН, 2012. – С. 13-14.

63. Шульц, В. Л. Информационное управление в условиях активного противоборства: модели и методы / В. Л. Шульц, В. В. Кульба, А. Б. Шелков, Д. А. Кононов, И. В. Чернов. – М.: Наука, 2011. – 187 с.

64. Шутов, А. Ю. Современная цивилизация: вызовы и альтернативы / А. С. Капто, А. Ю. Шутов; под. ред. А. Ю. Шутова; Сер. Библиотека факультета политологии МГУ. – М.: Изд-во Московского государственного университета, 2013. – 304 с.

Статьи:

65. Алексеева, И. Ю. Возникновение идеологии информационного общества / И. Ю. Алексеева // Информационное общество. – 1999. – Вып. 1. – С. 30-35.

66. Аникин, Л. С. Политика модернизации и информационное общество: социокультурный аспект / Л. С. Аникин, Ю. И. Тарский/ Власть. – 2012. – № 6. – С. 94-98.

67. Аничкина, Т. Б. О некоторых приемах «информационной войны США» / Т. Б. Аничкина // США – Канада. Экономика, политика, культура. – 2007. – № 7. – С. 123-127.

68. Арбатов, А. Г. Международная безопасность в эпоху перемен и внешняя политика России / А. Г. Арбатов // Россия в глобальном мире: 2000-2001. Хрестоматия в 6 тт.; под общ. ред. И. С. Иванова. – М.: Аспект Пресс. – 2012. – Т. 2. – С. 12.

69. Арбатов, А. Г. Угрозы реальные и мнимые. Военная сила в мировой политике начала XXI в. / А. Г. Арбатов // Россия в глобальной политике. – 2013. – Т. 11. – № 2. – С. 16.

70. Асланов, Р. М. Зарубежный опыт правового регулирования обеспечения информационной безопасности / Р. М. Асланов // Политика и общество. – 2012. – № 2(86). – С. 46.

71. Ачкасов, В. А. Кризис национальной идентичности и проблемы безопасности России / В. А. Ачкасов // Вестник Московского университета. Серия 12. Политические науки. – 2010. – № 4. – С. 63-67.

72. Ашманов И. С. Интервью Российской газете: Неделя № 6085 от 23 мая 2013 г.

73. Бакланов, П. Я. Об уникальности геополитического положения Тихоокеанской России / П. Я. Бакланов, М. Т. Романов // Проблемы Дальнего Востока. – 2013. – № 6. – С. 29-38.

74. Баклицкий, А. БРИКС и передовые технологии: перспективы сотрудничества и интересы России / А. Баклицкий, Е. Бужинский, О. Демидов, П. Лузгин, В. Орлов // Индекс безопасности. – 2013. – Т. 19. – № 4(107). – С. 86.

75. Баланс интересов в управлении [Электронный ресурс]. – Режим доступа: http://www.market-journal.com/voprosiupravleniya/79.html. (дата обращения: 11.12.2013)

76. Барановский, В. Г. Трансформация мировой системы в 2000-х гг. / В. Г. Барановский // Международные процессы. – 2010. – Т. 8. – № 1. – С. 3-13.

77. Бачило, И. Л. К вопросу о развитии информационного законодательства СНГ / И. Л. Бачило, М. А. Вус, О. С. Макаров // Информатизация и связь. – 2014. – № 1. – С. 13-16.

78. Беляев, И. И. Предпосылки к формированию комплексной системы международной информационной безопасности: доклад [Электронный ресурс] / И. И. Беляев // Материалы 16-го Национального форума информационной безопасности «Инфофорум-2014», Москва 30-31 января 2014 г. – Режим доступа: http://2014.infoforum.ru/conference/programma/ (дата обращения: 16.05.2012)

79. Бордюжа, Н. Н. Есть вещи, которые для нас запретны / Н. Н. Бордюжа // Коммерсантъ. – 2013. – 26 марта.

80. Братерский, А. В. Внешнеполитическая доктрина Обамы: постсоветский трек / А. В. Братерский // Международные процессы, 2013. – № 2. – С. 69-84.

81. Бродовская, Е. В. Политические функции Интернета в восприятии россиян / Е. В. Бродовская, В. Д. Нечаев // Городское управление. – 2013. – № 8. – С. 89-95.

82. Бронников, И. А. Интернет как ресурс политической власти / И. А. Бронников // Право и политика. – 2011. – № 6. – С. 1008-1018.

83. Буренок, В. М. О некоторых аспектах информационных войн / В. М. Буренок // Вооружение и экономика. – 2011. – № 3(15). – С. 5-16.

84. Васильева, Н. А. К вопросу о формировании внешнеполитической стратегии РФ / Н. А. Васильева // Актуальные проблемы мировой политики: сборник научных трудов. Выпуск 2; сост. В. С. Ягъя. – СПб.: Нестор-История, 2007.

85. Виноградов, А. В. Восток и Запад: ключи к политическим кодам / А. В. Виноградов // Мировые процессы. Журнал международной политики и международных отношений. – 2006. – Том 4. – № 1 (10). – С. 4-20.

86. Виноградова, С. М. Государство в современной информационно-политической системе / С. М. Виноградова, Г. С. Мельник // Вестник Санкт-

Петербургского университета. Серия 9: Филология. Востоковедение. Журналистика. – 2007. – № 4-1. – С. 115-131.

87. Владимирова, Т. В. Сетевые коммуникации как источник информационных угроз / Т. В. Владимирова // Социологические исследования. – 2011. – № 5. – С. 123-129.

88. Вус М.А. В интересах национальной и международной информационной безопасности / М.А. Вус, О.С. Макаров // Информатизация и связь.-2013.- № 6.

89. Выжутович, В. В. Роскошь как средство передвижения / В. В. Выжутович // Российская газета. – 2013. – 12 апреля. – № 80. – С. 3.

90. Гареев, М. А. Стратегическое сдерживание - важнейшее направление обеспечения национальной безопасности России в современных условиях / М. А. Гареев // Стратегическая стабильность. – 2009. – № 1. – С. 2-13.

91. Глазьев, С. Ю. Основа обеспечения экономической безопасности страны: альтернативный реформационный курс / С. Ю. Глазьев // Российский экономический журнал. – 1997. – № 1. – С. 8-9.

92. Глобальные процессы, безопасность и устойчивое развитие. Материалы «круглого стола» // Alma Mater. – 2012. – № 3. – С. 7-13.

93. Глущенко, Ю. Н. Стратегические риски России в условиях продолжающегося мирового экономического кризиса: нефтегазовый фактор / Ю. Н. Глущенко // Военно-политическая ситуация в мире и вопросы обеспечения национальной безопасности России; под ред. Г. Г. Тищенко и Е. С. Хотьковой. – М.: РИСИ, 2011. – С. 49-57.

94. Гомар, Т. Что скрывается за делом Сноудена? / Т. Гомар // Россия в глобальной политике. – 2013. – Т. 11. – № 5. – С. 86-93.

95. Гудев, П. А. Приоритеты США в Арктике / П. А. Гудев // Мировая экономика и международные отношения. – 2013. – № 9. – С. 49-60.

96. Гуменский, А. В. Управление международной информацией / А. В. Гуменский // Международные процессы. – 2010. – Т. 8. – № 1(22). – С. 31-43.

97. Гуторов, В. А. К вопросу о происхождении государства: парадоксы и

аномалии современных интерпретаций / В. А. Гуторов // Журнал «Полис». Политические исследования. – 2014. – № 3. – С. 91-110.

98. Дворкин, В. З. Трансформация стратегической стабильности / В. З. Дворкин // Мировая экономика и международные отношения. – 2013. – № 8. – С. 22-28.

99. Демидов, А. И. Политика и виртуальная среда / А. И. Демидов // Правовая политика и правовая жизнь. – 2012. – № 1. – С. 90-94.

100. Денежкина, И. Е. Система показателей для мониторинга экономической безопасности региона / И. Е. Денежкина, Д. А. Суздалева // Эффективное антикризисное управление. – 2011. – № 3(66). – С. 142-148.

101. Еляков, А. Д. Информационные технологии и современная война / А. Д. Еляков // Свободная мысль. – 2008. – № 1. – С. 181-194.

102. Еляков, А. Д. Проблемы информационной безопасности в использовании электронных компьютерных технологий / А. Д. Еляков // Социологические исследования. – 2013. – № 10. – С. 120-129.

103. Еремеев, С. Г. К проблеме актуализации политической власти как ценности в эпоху глобализации / С. Г. Еремеев // Вестник Московского университета. Серия 12. Политические науки. – 2012. – № 3. – С. 52-54.

104. Ерина, А. И. Интернет – политический ресурс воздействия на общественное мнение / А. И. Ерина // Обозреватель – Observer. – 2013. – № 1. – С. 94.

105. Ермаков, С. М. Трансформация НАТО после Лиссабонского саммита 2010 г.: от обороны территории к защите всеобщего достояния / С. М. Ермаков // Проблемы национальной стратегии. – 2011. – № 4. – С. 107-128.

106. Жарова, А. К. Сущность и структура информационного противоборства / А. К. Жарова // Государство и право. – 2009. – № 2. – С. 48-54.

107. Засурский, И. И. Общественное достояние и стратегия развития информационного общества / И. И. Засурский // Вестник Московского университета. Серия 10. Журналистика. – 2012. – № 3. – С. 7-15.

108. Зиновьева, Е. С. Международно-политические аспекты развития

Интернета / Е. С. Зиновьева // Вестник МГИМО-Университета. – 2013. – № 4. – С. 135-139.

109. Золотарев, П. С. Глобальное измерение войны / П. С. Золотарев // Россия в глобальной политике. – 2010. – № 1. – С. 45-58.

110. Золотарев, П.С. Цели и приоритеты военной политики России / П.С. Золотарев // Россия в глобальной порлитике.- 2007.- №2.- С. 76-87

111. Ибрагимова, Г. Р. Стратегия в области управления Интернетом и обеспечения информационной безопасности / Г. Р. Ибрагимова // Индекс безопасности. – 2013. – Т. 19. – № 1(104). – С. 181.

112. Иванов, И. С. Будущее – за «умной» внешней политикой / И. С. Иванов // Россия в глобальном мире: 2000-2001. Хрестоматия в 6 тт.; под общ. ред. И. С. Иванова. – М.: Аспект Пресс. – 2012. – Т. 1. – С. 24.

113. Иванов, И. С. Останется ли мир заложником ядерного оружия / И. С. Иванов // Международная жизнь. – 2013. – № 2. – С. 30-36.

114. Иванов, С. Б. Вооруженные силы России и ее геополитические приоритеты / С. Б. Иванов // Россия в глобальной политике. – 2004. – № 1. – С. 36

115. Иванов, С. Б. Структура и функции Совета национальной безопасности США / С. Б. Иванов // Зарубежное военное обозрение. – 2013. – № 4. – С. 13-17.

116. Извеков, Н. Н. Факторы, формирующие образ страны в окружающем мире / Н. Н. Извеков // Обозреватель – Observer. – 2010. – № 1. – С. 58.

117. Извеков, Н.Н. Проблема ограничения вооружений в XXI веке / Н.Н. Извеков // Обозреватель.-2008.-№2.-С. 74-81

118. Информационная война против России [Электронный ресурс]. – Режим доступа: http://schta.ru/index.php/history-rus/85-informack^naja-vojna-protiv-rossii (дата обращения: 21.11.2013)

119. Каберник, В. В. Проблемы классификации кибероружия / В. В. Каберник // Вестник МГИМО-Университета. – 2013. – № 2. – С. 72-77.

120. Камашев, С. В. Национальная безопасность и образование в условиях управляемого хаоса / С. В. Камашев // Философия образования. – 2013. – № 5. – С. 8-15.

121. Караганов, С.А. «Глобальный ноль» и здравый смысл / С.А. Караганов // Россия в глобальной политике.-2010.- №3.- С. 108-118

122. Караганов, С. А. Россия в мире: Противоречие противоречий / С. А. Караганов // Ведомости. – 2012. – 16 октября. – С. 4

123. Караяни А. И. Слухи как средство информационно-психологи-ческого противодействия / А. И. Караяни // Психологический журнал. – 2003. – Т. 24. – № 6. – С. 25.

124. Карпович, О. Г. Политика невоенного разрешения конфликтов / О. Г. Карпович //Закон и право. – 2012. – № 4. – С. 102-105.

125. Кибербезопасность РФ: щит и меч для защиты информации [Электронный ресурс]. – Режим доступа: http:// www.rusnevod.com/cgi-bin/rnev/ start.cgi?pm1=info2&grp=0208. (дата обращения: 12.02.2014)

126. Кларк, П. Обеспечение безопасности информационной магистрали. Как усовершенствовать системы электронной защиты США / П. Кларк, П. Левин // Россия в глобальной политике. – 2010. – Т. 8. – № 2. – С. 178.

127. Козин, В. П. «Новая» ядерная стратегия США и ее последствия для России / В. П. Козин // Международная жизнь. – 2013. – № 9. – С. 60-85.

128. Конституционно-правовой статус Совета Безопасности Российской Федерации / Под общ. ред. Н. П. Патрушева. – 2-е изд., испр. и доп. – М.: Изд-во «Известия», 2013. – С. 24-25, 27-28.

129. Кортунов, С. В. Мировая военно-политическая ситуация. Год 2025 / С. В. Кортунов // Международная жизнь. – 2010. – № 4. – С. 93-116.

130. Косов, Ю. В. Канал влияния. Почему «Аль-Джазира» побеждает конкурентов в информационной борьбе / Ю. В. Косов, С. А. Патаман // Санкт-Петербургские ведомости. – 2011. – 20 мая. – С. 4.

131. Косов, Ю. В. Международный терроризм как глобальная проблема / Ю. В. Косов // Социология войны и мира. Материалы «круглого стола» / Под ред. П. А. Цыганкова. – М.: Альфа-М. 2006. – С. 134-145.

132. Косов, Ю. В. Мировая политика и международные отношения / Ю. В. Косов // Политология: учебник для вузов / Под ред. М. А. Василика.–

М.: Гардарики, 2008. – С. 71, 165, 534-537.

133. Косов, Ю. В. Некоторые особенности интеграционных процессов на евразийском пространстве (На примере ЕврАзЭС и ШОС) / Ю. В. Косов, А. В. Торопыгин // Евразийская интеграция: экономика, право, политика. – 2011. – № 10. – С. 157-165.

134. Косов, Ю. В. Проблема безопасности государств - членов Евразийского экономического сообщества / Ю. В. Косов, А. В. Торопыгин // Управленческое консультирование. – 2005. – № 2. – С. 100-107.

135. Косолапов, Н. В. Безопасность международная, национальная, глобальная: взаимодополняемость или противоречивость? / Н. В. Косолапов // Мировая экономика и международные отношения. – 2006. – № 9. – С. 3-13.

136. Кочетков, А. П. Власть и элиты в глобальном информационном обществе / А. П. Кочетков // ПОЛИС. Политические исследования. – 2011. – № 5. – С. 8-20.

137. Кравченко, В. Ю. Стратегические приоритеты в сфере национальной безопасности [Электронный ресурс] / В. Ю. Кравченко, В. В. Щипалов // Аналитический вестник Совета Федерации ФС РФ. – 2010 г. – № 17 (403). С. 29

138. Красавин, И. В. Глобальная финансовая система в мировой политике: банки и оффшоры / И. В. Красавин // Негосударственные участники мировой политики / Под ред. М. М. Лебедевой, М. В. Харкевича. – М.: Аспект Пресс, 2013. – С. 20.

139. Кривошапка, И. Без страха перед рисками / И. Кривошапка // Эффективное антикризисное управление. – 2012. – № 4(73). – С. 5-10.

140. Крутских, А. В. К политико-правовым основаниям глобальной информационной безопасности / А. В. Крутских // Международные процессы. – 2007. – Т. 15. – № 1. – С. 28-37.

141. Крутских, А. В. Политико-правовой режим глобальной информационной безопасности / А. В. Крутских // Современная мировая политика / Отв. ред. А.Д. Богатуров. – М.: Аспект-Пресс, 2009. – С. 484-485.

142. Кузнецова, Н. А. Управление политической информацией и

манипуляция общественным сознанием / Н. А. Кузнецова // Власть. – 2011. – № 11. – С. 19-21.

143. Куликов, Е. М. Перспектива противодействия слухам в глобальной сети Интернет в целях обеспечения информационной безопасности / Е. М. Куликов // Власть. – 2011. – № 3. – С. 64-68.

144. Кучерявый, М. М. Геополитический анализ современных международных процессов и обеспечение национальной безопасности России в воздушно-космическом пространстве / М. М. Кучерявый // Известия РГПУ им. А.И. Герцена. – 2009. – № 12(89). – С. 95-101.

145. Кучерявый *М. М.* Геополитические противоречия между Россией и Западом в воздушно-космической сфере // Управленческое консультирование. 2009. № 1. С. 68-75.

146. Кучерявый, М. М. Космическое измерение военной безопасности Российской Федерации: геополитический анализ / М. М. Кучерявый // Власть. – 2009. – № 1. – С. 7-12.

147. Кучерявый, М. М. О совершенствовании и гармонизации национального законодательства государств-участников СНГ в сфере обеспечения информационной безопасности / М. М. Кучерявый, И. Л. Бачило, В. В. Бондуровский, М. А. Вус, О. С. Макаров // Информационное право. – 2013. – № 1(32). – С. 24-27.

148. Кучерявый, М. М. Проблемы обеспечения военной безопасности России в воздушном и космическом пространстве / М. М. Кучерявый // Личность. Культура. Общество. – 2009. – № 1. – С. 68-75.

149. Лавров, С. В. Пресс-конференция Министра иностранных дел России, посвященная итогам деятельности российской дипломатии в 2012 г. / С. В. Лавров // Международная жизнь. – 2013. – Февраль. – С. 2.

150. Ланцов, С. А. Безопасность государства-общества-человека в контексте противодействия терроризму / С. А. Ланцов // Вестник Московского университета. Серия 12. Политические науки. – 2010. – № 4. – С. 58-62.

151. Ланцов, С. А. Теоретические концепции международной интеграции и перспективы интеграционных процессов на постсоветском пространстве / С. А. Ланцов // Вестник Санкт-Петербургского университета. Серия 6: Философия. Культурология. Политология. Право. Международные отношения. – 2013. – № 2. – С. 65-74.

152. Лебедева, М. М. Акторы современной мировой политики: тренды развития / М. М. Лебедева // Вестник МГИМО-Университета. – 2013. – № 3 (28). – С. 38-42.

153. Левкин, И. М. Основные проблемы информационно-экономической безопасности Российской Федерации на современном этапе / И. М. Левкин, С. Ю. Микадзе // VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2013 г.: Материалы конференции / СПОИСУ. – СПб., 2013. – С. 176-177.

154. Лузянин, С. Г. ШОС: проблемы безопасности и перспективы сотрудничества в Евразии / С. Г. Лузянин // Проблемы Дальнего Востока. – 2011. – № 1. – С. 15.

155. Лукин А. В. Шовинизм или хаос: порочный выбор для России / А. В. Лукин // Журнал Полис: Политические исследования. – 2014. – № 3. – С. 159-172.

156. Луков, В. Б. Россия в «Большой восьмерке»: из гостей в председатели / В. Б. Луков // Россия в глобальном мире: 2000-2001. Хрестоматия в 6 тт.; под общ. ред. И. С. Иванова. – М.: Аспект Пресс. – 2012. – Т. 1. – С. 262-274.

157. Луппов И. Ф. Современный терроризм как политический феномен / И. Ф. Луппов // Известия Российского государственного педагогического университета им. А.И.Герцена. – 2009. – № 103. – 225-231.

158. Макаренкова, И. В. Современные зарубежные концепции национальной безопасности [Электронный ресурс]/ И. В. Макаренкова // Аналитический вестник Совета Федерации ФС РФ. – 2010. –№ 17(403). – Режим доступа: http://www.budgetrf.ru/Publications/Magazines/VestnikSF/2010/VSF_NEW201009161033/VSF_NEW201009161033_000.html. (дата обращения: 05.12.2013)

159. Малюк, А. А. Формирование культуры информационной безопасности общества / А. А. Малюк // Педагогика. – 2009. – № 3. – С. 33.

160. Манойло А.В, Модели информационно-психологического управления международными конфликтами / А.В. Манойло // Вестник Моск. Ун-та. Серия 12. Политические науки.-2012.-№2.- С. 85-95

161. Марков, А. А. Характеристики информационной безопасности на современном этапе развития общества / А. А. Марков // Управленческое консультирование. – 2010. – № 3. – С. 70-71.

162. Материалы Международной конференции «Ядерное оружие и международная безопасность в XXI в.» / Гл. ред. И. С. Иванов. – М.: Спецкнига, 2012. – С. 16.

163. Материалы международной научно-практической конференции на тему: «Суверенитет государств и концепция «ответственности по защите»: эволюция международной ситуации и интересы России», 30 октября 2013 г. http://www.dipacademy.ru/31.10.13.shtml (дата обращения: 12.11.2013)

164. Мендкович, Н. Есть еще порох в пороховницах? [Электронный ресурс] / Н. Мендкович // Российский совет по международным делам (РСМД), 25 февраля 2013 г. – Режим доступа: http://russiancouncil.ru/inner/ ?id_4=1440#top. (дата обращения: 24.05.2014)

165. Мендкович, Н. Ирак: десять лет спустя [Электронный ресурс] / Н. Мендкович // Российский совет по международным делам (РСМД), 23 марта 2013 г. – Режим доступа: http://russiancouncil. ru/inner/?id_4=1584#top. (дата обращения: 25.05.2013)

166. Метаморфозы мировой политики / Под общ. ред. М. М. Лебедевой. – М.: МГИМО-Университет, 2012. – С. 10, 17-18.

167. Мизин, В. И. Новые аспекты стратегии национальной безопасности / В. И. Мизин // Вестник МГИМО-Университета. – 2012. – № 6(27). – С. 26.

168. Мизин, В. И. Российско-американский диалог по контролю над вооружениями / В. И. Мизин // Международная жизнь. – 2013. – № 9. – С. 86-98.

169. Михайленок, О. М. Национальный суверенитет и российский

федерализм / О. М. Михайленок // Власть. – 2010. – № 3. – С. 4-8.

170. Михайленок, О. М. Стратегическая культура как системообразующий фактор общественно-политического согласия / О. М. Михайленок // Россия реформирующаяся. Выпуск 11: Ежегодник / Отв. ред. М. К. Горшков. – М.: Новый хронограф, 2012. – С. 125-141.

171. Модестов, С. А. Стратегическое сдерживание на театре информационного противоборства/ С. А. Модестов // Вестник Академии военных наук. – 2009. – № 1. – С. 33-36.

172. Назарчук, А. В. Сетевое общество и его философское осмысление / А. В. Назарчук // Вопросы философии. – 2008. – № 7. – С. 61-75.

173. Новацкий, А. Борьба вокруг проекта Конвенции ООН о международной информационной безопасности [Электронный ресурс] / А. Новацкий // Фонд стратегической культуры. – Режим доступа: http://www.fondsk.ru/pview/2012/07/14/borba-vokrug-proekta-konvencii-oon-o-mezh-dunarodnoj-informacionnoj-bezopasnosti-15499.html. (дата обращения: 21.11.2013)

174. Новикова, И. И. Стратегия информационного развития и национальной безопасности России / И. И. Новикова // Власть. – 2009. – № 2. – С. 44.

175. Ноговицын, А. А. Методика оценки и пути обеспечения военной безопасности государства / А. А. Ноговицын, В. В. Барвиненко, Ю. И. Мушков // Вестник Академии военных наук. – 2004. – № 1(6). – С. 115.

176. Носов, Е. Власть вещей. Человечество стоит на пороге создания информационной среды, в которой гомо сапиенс будет лишним / Е. Носов // Итоги. – 2013. – 23 декабря. -№51(915). – С. 56.

177. Панкова, Л. В. Военно-экономическое обеспечение безопасности: инновационное измерение / Л. В. Панкова // Вестник Московского университета. Серия 25. Международные отношения и мировая политика. – 2012. – № 2. – С. 23.

178. Панкратов, С. А. Глобальные и региональные факторы политического риска государственному режиму в условиях реализации национальной модели модернизации [Электронный ресурс] / С. А. Панкратов, И. М. Соколов // Теория и практика общественного развития. – 2012. – № 2. – Режим доступа: http://teoria-

practica.ru/rus/files/arhiv_zhurnala/2012/2/politika/pankra-tov-sokolov.pdf. (дата обращения: 19.11.2013)

179. Панцерев, К.А. Информационное общество: эволюция концепции в исторической перспективе / К. А. Панцерев // Вестник Санкт-Петербургского Университета. Серия 6. Философия. Культурологи. Политология. Право. Международные отношения. – 2010. – Вып.1. – С. 65-72.

180. Патрушев, Н. П. ФСБ раскинет сеть / Н. П. Патрушев // Российская газета. – 2013. – 20 февраля. – № 36(6012). – С. 17.

181. Пахарева, Е. Н. Защита пользователей от распространения контента террористического характера в сети Интернет: политологический аспект проблемы / Е. Н. Пахарева // Социальная политика и социология. – 2010. – № 2. – С. 82.

182. Пашков, В. Информационная безопасность США / В. Пашков // Зарубежное военное обозрение. – 2010. – № 10. – С. 3-13.

183. Пентагон борется с виртуальными врагами [Электронный ресурс]. – Режим доступа: http://www.newsru.com/world/19sep2007/kiber.html. (дата обращения: 13.03.2014)

184. Песков рассказал о чрезвычайной цензуре в Европе [Электронный ресурс]. – Режим доступа: http://mformmg.ru/2014/04/16/peskov-rasskazal-o-chrezvychaynoy-cenzure-v-evrope.html. (дата обращения: 21.09.2013)

185. Петров, Н. Жизнь после «Твиттера». Почему Эрдоган пока не повторил судьбу Януковича / Н. Петров // Русский репортер. – 2014. – 3-10 апреля. – № 13(341). – С. 36-37.

186. Поздняков, А. И. Критерии оценки эффективности обеспечения национальной безопасности [Электронный ресурс] / А. И. Поздняков // Аналитический вестник Совета Федерации ФС РФ. – 2010. – № 17(403). – Режим доступа:
http://www.budgetrf.ru/Publications/Magazines/VestnikSF/2010/VSF_NEW20100916 1033/VSF_NEW201009161033_000.html. (дата обращения: 10.12.2013)

187. Понеделков, В. В. Региональные административно-политические элиты

России: итого постсоветской эволюции / В. В. Понеделков, В. Д. Лысенко // Социология власти. – 2012. – № 3. – С. 30-39.

188. Прокопов, Б. И. Сущность и содержание экономической безопасности / Б. И. Прокопов // Проблемы современной экономики. – 2008. – № 4 (28). – С. 44-148.

189. Развитие отрасли инфокоммуникационных технологий (ИКТ) в России [Электронный ресурс] // CRN ИТ-БИЗНЕС. – 2012. – 01 августа. – Режим доступа: http://www.crn.ru/news/detail_print. php?ID=68520&print=Y. (дата обращения: 29.11.2013)

190. Рогов, А. С. Государственная безопасность: элемент или сдерживание национальной безопасности Российской Федерации / А. С. Рогов, Ю. Г. Федотова // Власть. – 2013. – № 12. – С. 128-132.

191. Рогов, С. М. Стратегическое одиночество России [Электронный ресурс] / С. М. Рогов // Экономические стратегии. – 2004. – № 4. – С. 12–17. – Режим доступа: http://www.tinlib.ru/istorija/besedy/p11.php. (дата обращения: 25.11.2012)

192. Роговский, Е. А. Американская стратегия информационного преобладания [Электронный ресурс] / Е. А. Роговский // Россия и Америка в XXI в.: электронный научный журнал. – 2009. – № 3. – Режим доступа: http:// www.msus.rn/?act=read&id=161. (дата обращения: 20.11.2013)

193. Рогозин, А. Д. «Общественная дипломатия» НАТО: информационная безопасность России / А. Д. Рогозин // Власть. – 2008. – № 9. – С. 32.

194. Рогозин, Д. О. Свой чип карман не тянет / Д. О. Рогозин // Российская газета. – 2014. – 15 августа. – № 184(6456). – С. 5.

195. Россия заняла 31-е место в интернет-рейтинге [Электронный ресурс]. – Режим доступа: http://www.sostav.ru/news/2012/09/06/rossiya_31_mesti _intemet_reyting. (дата обращения: 06.09.2012)

196. Савельев, А. Г. Роль ядерного оружия в обеспечении безопасности РФ / А. Г. Савельев // Военно-политическая ситуация в мире и вопросы обеспечения национальной безопасности России / Под ред. Г. Г. Тищенко и Е. С. Хотьковой. –

М.: Рос. ин-т стратегич. исслед., 2011. – С. 62.

197. Самуйлов, С. М. Вторжение США в Ирак / С. М. Самуйлов // Свободная мысль. – 2012. – Июнь. – №№ 3-4. – С. 54.

198. Санина, А. Г Информационное общество и государственная идентичность / А. Г. Санина // Информационное общество. – 2013. – № 6. – С. 9-15.

199. Сараев, В. Когда данные стали большими / В. Сараев // Эксперт. – 2013. – 13-19 мая. – № 19. – С. 51-54.

200. Севастьянов, С. В. «Новый регионализм» Восточной Азии: теоретические и практические аспекты / С. В. Севастьянов // Журнал «Полис»: Политические исследования. – 2009. – № 4. – С. 111-122.

201. Сергунин, А. А. Международная безопасность: новые подходы и концепты / А. А. Сергунин // Журнал «Полис»: Политические исследования. – 2005. – № 6. – С. 130.

202. Сергунин, А. А. Суверенитет: эволюция концепта [Электронный ресурс] / А. А. Сергунин // Политэкс. – 2010. – № 4. – С. 23-28. – Режим доступа: http://www.politex.info/content/view/756/30/. (дата обращения: 10.03.2014)

203. Сергунин, А. А. Суверенитет: современные дискуссии в теории международных отношений / А. А. Сергунин // Научные ведомости Белгородского госуниверситета. Серия История. Политология. Экономика. Информатика. – 2010. – № 19(90). – Выпуск 16. – С. 231-236.

204. Сивоволов, Д. Л. Роль российской дипломатии в построении «электронного государства» в Российской Федерации / Д. Л. Сивоволов // Вестник МГИМО-Университета. – 2013. – № 5. – С. 54-57.

205. Слипченко, В. И. Информационное противоборство в бесконтактных войнах [Электронный ресурс] / В. И. Слипченко. – Режим доступа http://viperson.ru/wind.php?ID=291897&soch=1. (дата обращения: 11.04.2013)

206. Смирнов, А. А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского союза / А. А. Смирнов. – М.: ЮНИТИ. ДАНА: Закон и право, 2012. – С. 77-110.

207. Смирнов, А. И. Глобальная безопасность и «Мягкая сила 2.0»: вызовы и возможности для России / А. И. Смирнов, И. Н. Кохтюлина. – М.: ВНИИгеосистем, 2012. – С. 58,72.

208. Смирнов, В. М. Космос в вопросах сооруженной борьбы / В. М. Смирнов // Национальная оборона. – 2008. – № 7.

209. Согрин, В. В. Меняющееся восприятие США в постсоветской России / В. В. Согрин // Общественные науки и современность. – 2013. – № 6. – С. 121-133.

210. Соколов, М. На страже безопасности. Оборонно-промышленный комплекс России перестроится на отечественные информационные технологии / М. Соколов // Российская газета. – 2014. – 28 мая. – № 118(6390). – С. 4.

211. Солодовников, А. Д. К вопросу о проблеме информационной безопасности контекста национальных информационных интересов / А. Д. Солодовников // Социально-гуманитарные знания. – 2011. – № 2. – С. 327.

212. Стариков, Н. В. Дефицит Государственного Суверенитета [Электронный ресурс] / Н. В. Стариков. – Режим доступа: http://nstarikov. livejournal.com/139747.html. (дата обращения: 19.05.2013)

213. Старостина, Е. Терроризм и кибертерроризм: угроза международной безопасности [Электронный ресурс] / Е. Старостина // Центр исследования компьютерной преступности: интернет-издание. – Режим доступа: http://www.crime-research.ru/articles/starostina. (дата обращения: 17.04.2013)

214. Степенцев, В. Клик победы / В. Степенцев // Вокруг света. – 2013. – № 6(2873). – С. 36.

215. Степин, В. С. Современное общество: общество риска, информационное общество, общество знаний / В. С. Степин, Г. Бехман // Вопросы философии. – 2010.– № 7. – С. 165-167.

216. Стрельцов, А. А. Обеспечение информационной безопасности России. Теоретические и методологические основы / А. А. Стрельцов: из серии монографий под общ. ред. В. А. Садовничего и В. П. Шерстюка «Научные проблемы безопасности и противодействия терроризму». – М.: МЦНМО, 2002. – 86 с.

217. Струговец, В. Перспективные направления информационной политики

ОДКБ / В. Струговец // Власть. – 2011. – № 8. – С. 98.

218. Сундиев, И. Сетевые возможности и сетевые угрозы / И. Сундиев, А. Смирнов // Свободная мысль. – 2013. – № 5. – С. 191-204.

219. Супрун В. Н. Теоретико-правовые основы информационного суверенитета. – Дис. на соискание научной степени канд. юрид. наук. – Харьковский национальный университет внутренних дел, Харьков, 2010.

220. Сурма, И. В. Глобальный наднациональный фактор международных отношений и его социальная философия / И. В. Сурма // Вестник МГИМО-Университета. – 2013. – № 4. – С. 141-150.

221. Суханов, С. А. Угрозы безопасности России растут. Роль и место ракетно-космической обороны страны в парировании возможного нападения / С. А. Суханов, В. П. Омельчук, В. Ф. Фатеев // Воздушно-космическая оборона. – 2006. – №4(29). – С. 28-31.

222. США тайно финансировали «кубинский Twitter», чтобы распространять пропаганду [Электронный ресурс]. – Режим доступа: http://russian.rt.com/article/26356. (дата обращения: 15.05.2013)

223. Сюн, Гуанкай. Всеобъемлющая концепция национальной безопасности Китая / Гуанкай Сюн // Россия в глобальной политике. – 2010. – Т. 7. – № 3. – С. 92-98.

224. Тарасов, Е. Информационная безопасность США в опасности [Электронный ресурс] / Е. Тарасов. – Режим доступа: http://newsland.com/news/detail/id/1207288. (дата обращения: 18.01.2014)

225. Топорая, Г. БРИКС: попытка согласования долгосрочной стратегии [Электронный ресурс] / Г. Топорая. – Режим доступа: http:// russian-council.ru/inner/?id_4=1506#top. (дата обращения: 15.10.2013)

226. Торопыгин, А.В. Парламентская дипломатия в структуре многосторонних международных отношений (На примере деятельности Постоянной комиссии МПА ЕврАзЭС по торговой политике и международному сотрудничеству)/ И.В. Карпенко, А.В. Торопыгин // Евразийская интеграция: экономика, право, политика № 7 - 2010.-С. 150-154

227. Турецкая республика [Электронный ресур] // Портал внешнеэкономической информации. Министерство внешнеэкономического развития Российской Федерации. – Режим доступа: //http://www.ved.gov.ru/exportcountries/tr/about_tr/review_tr. (дата обращения: 21.02.2014)

228. Турко, Н. И. Системология региональной безопасности. Геополитическое эссе / Н. И. Турко. – М., 2000.

229. Туронок, С. Г. Информационный терроризм: выработка стратегии противодействия / С. Г. Туронок // Общественные науки и современность. – 2011. – № 4. – С. 131-140.

230. Фененко, А. «Белый дом подчеркнул свое нежелание вести диалог с администрацией Владимира Путина» [Электронный ресурс] / А. Фененко. – Режим доступа: http://russiancouncil.ru/blogs/debate/?id_4=614. (дата обращения: 12.03.2014)

231. Фокина, В. В. СМИ как акторы мировой политики / В. В. Фокина // Вестник МГИМО-Университета. – 2013. – № 1(28). – С. 61, 65.

232. Фролов, Д. Б. Информационная геополитика и вопросы информационной безопасности / Д. Б. Фролов // Национальная безопасность. – 2009. – № 1. – С. 72–79.

233. Хайнс, С. Договор о торговле оружием: далек от совершенства, но лучше чем ничего [Электронный ресурс] / С. Хайнс // Российский совет по международным делам (РСМД), 18 апреля 2013 г. – Режим доступа: http://russiancouncil.ru/inner/?id_4=1730#top. (дата обращения: 07.02.2014)

234. Хрыков, В. П. Информационное общество в России: условия и проблемы формирования / В. П. Хрыков // Политика и общество. – 2011. – № 6. – С. 18-25.

235. Худикова, Л. Опрос россиян о присоединении Крыма. Цифры – фантастические [Электронный ресурс] / Л. Худикова // Россия 24. Вести. – 2014. – 17 марта.– Режим доступа: // http://www.vesti.ru/doc.html?id=1385156 (дата обращения: 26.02.2014)

236. Цветкова, Н. А. Информационная война талибов: Вашингтон в обороне

/ Н. А. Цветкова // Азия и Африка сегодня. – 2013. – № 1. – С. 10-16.

237. Чельцов, Б. Ф. Вопросы воздушно-космической обороны в военной доктрине России / Б. Ф. Чельцов // Военная мысль. – 2007. – №4. – С. 5-10.

238. Черненко, Е. Джон Керри согласовал соглашения. К июньской встречи президентов РФ и США будут подготовлены пять документов / Е. Черненко, И. Сафронов // Коммерсантъ. – 2013. – 8 мая. – № 78. – С. 6.

239. Чуркин, В. И. ООН – непревзойденный игрок на мировом поле / В. И. Чуркин // Международная жизнь. – 2010. – № 9. – С. 78.

240. Шабров, О. Ф. Государство в глобализующемся мире: испытание постмодерном / О. Ф. Шабров // Власть и политика: институциональные вызовы XXI века. Политическая наука: Ежегодник 2012 / Российская ассоциация политической науки; гл. ред. А. И. Соловьев. – М.: Российская политическая энциклопедия (РОССПЭН), 2012. – С. 87-101.

241. Шадрина, Т. Невыносимая локальность сети / Т. Шадрина // Российская газета. – 2014. – 18 февраля. – № 37(6309). – С. 1, 9.

242. Шаклеина, Т. А. Американские концепции статус-кво и современного миропорядка / Т. А. Шаклеина // Современная мировая политика. Под ред. А. Д. Богатурова. – М.: АСПЕКТ ПРЕСС, 2010. – С. 202-214.

243. Шаклеина, Т. А. Общность и различия в стратегиях России и США / Т. А. Шаклеина // Международные процессы. – 2013. – № 2. – С. 6-19.

244. Шариков, П. А. В бой идут кибервойска / П. А. Шариков // Независимое военное обозрение. – 2012. – 13 апреля. – С. 4.

245. Шариков, П. А. Эволюция государственной стратегии в сфере информационной безопасности / П. А. Шариков // США – Канада. Экономика, политика, культура. – 2009. – № 12. – С. 95-108.

246. Шариков, П. А. Подходы демократов и республиканцев к информационной безопасности [Электронный ресурс] / П. А. Шариков // Россия и Америка в XXI в.: электронный научный журнал. – 2012. – № 1. – Режим доступа: http://www.rusus.ru/?act=read&id=312. (дата обращения: 11.11.2013)

247. Шевченко, А. В. Управление безопасностью информационных

процессов / А. В. Шевченко. – М.: Изд-во РАГС, 2009. – С. 84.

248. Шестаков, Е. Мир становится все менее прозападным: интервью с С. Карагановым [Электронный ресурс] / Е. Шестаков // Российская газета. – 2014.– 24 апреля. – № 93(6365). – С.1, 7, 10

249. Шестаков, Е. Сила есть. Ума бы надо / Е. Шестаков // Российская газета. – 2014. – 14 апреля. – № 84(6356). – С. 7.

250. Шеховцев, Н. П. Информационное оружие: теория и практика применения в информационном противоборстве / Н. П. Шеховцев, Ю. П. Кулешов // Вестник Академии военных наук. – 2012. – № 1(38). – С. 35-40.

251. Шинкарецкая, Г. Г. Международно-правовые проблемы враждебного воздействия на информационные системы / Г. Г. Шинкарецкая // Государство и право. – 2013. – № 9. – С. 82-88.

252. Шишкина, О. В. Внешнеполитические ресурсы: Россия и ЕС на пространстве «общего соседства» / О. В. Шишкина. – М.: Аспект Пресс, 2013. – С. 16, 25.

253. Шомова, С. А. СМИ или медиа? (К вопросу об определении понятий) / С. А. Шомова, Т. Б. Тихомирова // Россия: на пути глобализации и интеграции: Научные труды ИМПЭ им. А.С. Грибоедова. К 20-летию Института международного права и экономики имени А. С. Грибоедова. Вып. 2012. – М.: Издательский дом «Буквовед», 2012. – С. 260-264.

254. Щербович, А. А. Ограничения свободы слова в Интернете в целях защиты нравственности и здоровья граждан / А. А. Щербович // Политика и общество. – 2011. – № 4. – С. 126-132.

255. Юрьева, Т. В. Проблемы региональной безопасности: современный опыт Европы / Т. В. Юрьева // Вестник МГИМО-Университета. – 2010. – № 6. – С. 127, 130.

256. Юсупов, Р. М. Информационная безопасность и кибербезопасность: семантический конфликт и сосуществование / Р. М. Юсупов, В. М. Шишкин // Информатизация и связь. – 2013. – № 6. – С. 22-27.

257. Юсупов, Р. М. Эскиз системного подхода к формированию понятийного аппарата информационной безопасности / Р. М. Юсупов, М. А. Вус, М. М. Кучерявый и др. // Информатизация и связь. – 2012. – № 9. – С. 7-15.

258. Ягья, В. С. Балтинизация в контексте глобализации и регионализации мировой политики / В. С. Ягья // Россия и мир: опыт и проблемы модернизации. – СПб.: СПбГУТД, 2011. – С. 304-309

Авторефераты диссертаций:

259. Арапова, Н. П. Социально-информационный подход в теории информационных войн: дис. ... канд. полит. наук: 10.01.10 / Арапова Наталия Павловна. – М., 2003. – 181 с.

260. Кучерявый, М. М. Система обеспечения национальной безопасности Российской Федерации в воздушно-космическом пространстве: политологический анализ: дис. ... канд. полит. наук: 23.00.02 / Кучерявый Михаил Михайлович. – СПб. 2009. – 219 с.

Публикации на иностранных языках:

261. Beck U. From Industrial Society to the Risk Society // Theory, Culture and Society, February 1992. V. 9. No.1. P. 97-123.

262. Bell D. The coming of post-industrial society: A venture of social forecasting. N.Y.: Basic Books. 1973.

263. Held D., McGrew A., Goldblatt D., Perraton J. Global Transformation. Politics, Economics and Culture. Cambridge.: Polity Press, 2000. 515 p.

264. Human Developement Report. UNDP. N. Y.: Oxford University Press, 1994.

265. Masuda Y. The Information Society as Postindustrial Society. Wash.: World Future Soc., 1983. 299 p.

266. Microelectronics and Society: For Better or For Worse. A Report to the Club of Rome / Ed. by G. FRriedrichs and A. Shaff. Oxford etc.: Pergamon Press. 1982. XII. 353 p.

267. National Secutity Strategy. May 2010. P. 4-5 // URL: http:// nssarchive.us/ NSSR/2010.pdf.

268. Scholte J. A. Globalization: A Critical Introduction. N.Y.: Palgrave Macmillan, 2005. 492 p.

269. Top 20 Countries with the Highest Number of Internet Users // URL: http://www.intemetworldstats.com/top20.htm. (дата обращения: 22.06.2013)