**Информационная безопасность Российской Федерации**

Дипломная работа

Юспа Михаил Михайлович

Белорусский государственный университет

Минск – 2007

**Введение**

Проблема обеспечения информационной безопасности любого государства является одним из наиболее важных аспектов его внешней политики, так как именно информационная сфера представляется на сегодняшний день важнейшим объектом приложения деятельности различных участников международных отношений. Каждый из них стремится не только сформировать и поддержать благоприятный имидж в мировой политике, но и взять под контроль важнейшие информационные ресурсы, в первую очередь, средства массовой и сетевой информации, функционирование которых в значительной степени определяют мировое общественное мнение.

Особенное значение обеспечению информационной безопасности придают те страны, которые являются либо претендуют на роль великих держав. Правительства таких государств осознают, что без учета информационного фактора они не смогут защищать свои геополитические интересы, оказывать воздействие на внешнюю политику других стран, определять основные направления политического развития отдельных регионов и влиять на мировую политику в целом. В полной мере это утверждение относится к внешнеполитическому курсу такого влиятельного государства, как Российская Федерация, руководство которой также уделяет большое внимание вопросам собственной информационной безопасности и разработке комплексной системы ее реализации.

Необходимость рассмотреть ключевые направления такой деятельности и дать общую оценку места и роли современной России в глобальном информационном обществе определяет актуальность темы данного исследования. Эта проблема приобретает особую важность, учитывая теснейшее сотрудничество между Республикой Беларусь и Российской Федерацией в рамках построения Союзного Государства.

Научная значимость рассматриваемой темы обусловлена неотложностью ее изучения в Республике Беларусь, так как проблема формирования информационной безопасности нашей страны, разработка новейших методов реализации этой задачи, а также их адаптация к меняющимся условиям современных международных отношений является сегодня важнейшей задачей для специалистов в области мировой политики, политологии и социологии.

Практическая значимость изучения информационной безопасности Российской Федерации может быть, в первую очередь, обоснована целым рядом общих для Беларуси и России угроз в политической, экономической и гуманитарной сферах. Такие риски, как усиление радикальных политических течений, вопросы энергетической безопасности, конкуренция на внешних рынках, глобальные социальные угрозы и многие другие в равной степени значимы в настоящее время как для Республики Беларусь, так и для Российской Федерации. Поэтому анализ обеспечения информационной безопасности России на современном этапе позволит в дальнейшем сформулировать наиболее оптимальную модель защиты информационной безопасности нашей страны и определить основные направления ее реализации.

Исходя из этого, предметом исследования в данной работе является информационная безопасность Российской Федерации начиная с 1992 года и до настоящего времени.

Цель работы – проанализировать основные подходы к обеспечению этого вида безопасности в России в условиях современных международных отношений.

В качестве важнейших задач работы необходимо указать следующие:

1. Рассмотреть основные принципы государственной информационной политики Российской Федерации как составного элемента российского внешнеполитического курса;

2. Проанализировать действия и шаги, предпринятые Правительством Российской Федерации в области государственной информационной политики в указанный выше период;

3. Дать прогноз относительно дальнейших изменений концепции информационной безопасности России с учетом новых рисков и угроз.

Необходимо обратить внимание на то, что данная проблематика еще недостаточно полно освещена в научной литературе, поскольку само понятие «информационная безопасность» появилось сравнительно недавно в связи с усилением значения новых информационных технологий и их интенсивным применением при решении различных внешнеполитических задач.

Исходя из этого, существует и небольшое число публикаций, в которых поднимается изучаемый в данной работе комплекс вопросов. Поэтому именно это обстоятельство вызвало наибольшие трудности в ходе ее подготовки и обусловило соответствующее количество использованных источников и публикаций.

Среди белорусских авторов, которыми затрагивались вопросы информационной безопасности, следует, прежде всего, упомянуть доктора юридических наук, профессора С.А. Трахименка. Этот исследователь рассмотрел методолого-правовые аспекты безопасности государства на современном этапе, среди которых выделил информационную составляющую как одну из ключевых в условиях возрастания роли информационных технологий [21].

Важное значение при подготовке данной работы имело также изучение опыта реализации государственной информационной политики в странах АТР и его сопоставление с российской моделью. Обстоятельный анализ азиатского подхода к решению проблемы обеспечения информационной безопасности изложен, в частности, в монографии доктора политических наук, профессора Ю.И. Малевич [13]. Проблемы так называемого цифрового неравенства в регионе Ближнего и Среднего Востока касается в своей статье Р. М. Турарбекова [22].

Одним из ведущих российских исследователей в данной области является специалист в сфере новейших информационных технологий, автор монографии «Становление глобального информационного общества», профессор А.А. Чернов [27]. Определенный вклад в изучение указанной проблематики внес также профессор Санкт-Петербургского университета, автор монографии «Политическая коммуникация в информационном обществе» М.С. Вершинин [4].

Помимо этого, необходимо назвать таких белорусских и российских авторов, как Алпатов В.М., Крысько В.Г., Удовик С.Л, Уткин А.И., Федотова Л.Н. и др., в работах которых освещены некоторые аспекты изучаемой темы [12, 8, 23-25]. Помимо этого, анализ состояния научных исследований, проведенный секцией по информационной безопасности научного совета при Совете Безопасности Российской Федерации, позволил определить приоритетные проблемы научных исследований в области информационной безопасности, на решении которых рекомендовано сосредоточить внимание организациям РАН, научным учреждениям федеральных органов исполнительной власти. Эти проблемы имеют междисциплинарный характер и для их решения необходимы исследования в различных отраслях научных знаний: философии, социологии, психологии, политологии, юридических и технических науках. Кроме того, необходима концепция «информации», адекватная междисциплинарному характеру проблем обеспечения информационной безопасности.

Среди ученых, работающих в этих областях, можно отметить: Смоляна Г.Л., Хачатурова К.А., Цыгичко В.Н., Черешкина Д.С., Яковенко А.В., которые исследуют политологические проблемы обеспечения информационной безопасности [26; 29-30]; А. В. Брушлинского, Грачева Г.В., Лепского В.Е., Мельника И.К. [6-7; 17], которые рассматривают различные аспекты защиты психической деятельности человека от вредного информационного воздействия; Расторгуева С.П. и Почепцова Г.Г. [15; 18-20], исследующих вопросы информационных войн; Войскунского А.Е., исследующего проблемы воздействия Интернета на развитие личности [9]. Вместе с тем, данная проблема требует более детального и комплексного анализа, учитывая целый ряд новых факторов политического и экономического характера, которые оказывают непосредственное воздействие на место и роль России в мировом информационном пространстве.

Источниковой базой для написания работы послужили законодательные акты Российской Федерации, которые регулируют различные аспекты государственной информационной политики России на современном этапе. Среди них необходимо, в первую очередь, назвать Доктрину информационной безопасности Российской Федерации, утвержденную президентом РФ В. Путиным 9 сентября 2000 г., а также Закон Российской Федерации «О безопасности» от 5 марта 1992 и Концепцию государственной информационной политики РФ, одобренную Комитетом по информационной политике и связи Государственной Думы Федерального Собрания РФ 21 декабря 1998 г., и Концепцию формирования информационного общества в России, одобренную Государственной комиссией по информатизации при Государственном комитете РФ по связи и информатизации 28 мая 1999 г. [2, 10-11].

Структура работы соответствует поставленным целям и задачам.

В первой главе рассматриваются основные принципы государственной информационной политики Российской Федерации в контексте современного внешнеполитического курса этого государства. Вторая глава посвящена анализу политико-правовой основы обеспечения информационной безопасности России, которая является основным базовым документом в указанной области. В заключении изложены результаты работы.

**Глава 1. Основные принципы государственной информационной политики Российской Федерации**

Информационное противоборство на рубеже ХХ-XXI вв. явилось одной из важнейших составляющих современной мировой политики. Проиграв информационное противостояние в борьбе с США, СССР распался, биполярная система сменилась на американскую гегемонию, а мировое сообщество убедилось, что победу американцев в холодной войне обеспечили не только современные виды вооружения или экономическое преимущество, но и умелое использование новейших информационных технологий.

Вместе с тем, на современном этапе информационная монополия США представляется отнюдь небесспорной, учитывая активное стремление многих других государств бросить Вашингтону геополитический вызов. В качестве идеологической основы для нового конфликта используется фактор так называемого цифрового неравенства, которое характерно сегодня для многих регионов мира.

Так, известный российский исследователь А.А. Чернов обращает внимание на то обстоятельство, что уже в настоящий момент 4,8 млрд. чел. из 6 млрд. проживает в условиях бедности, а это означает, что они не могут воспользоваться современными информационными технологиями. В ближайшие годы к ним прибавится еще 2 млрд. чел. Более того, в то время как интеллектуальная элита мира и аналитики обсуждают перспективы формирования глобального информационного общества, треть населения планеты никогда не пользовались обычным телефоном [27, c. 75].

Нельзя не отметить, что страны большой «восьмерки» предпринимают определенные меры для того, чтобы преодолеть цифровое неравенство. В частности, в 2000 г. на саммите в Окинаве была принята Хартия глобального информационного общества, в которой предусматривалось, что промышленно развитые страны берут на себя обязательство оказать помощь бедным государствам и предоставить им доступ к новым информационным технологиям [14].

Несмотря на то, что этот документ появился на свет шесть лет назад, существенных успехов в его реализации достигнуто не было, и бедные государства по-прежнему остались «на обочине» развития единого мирового информационного пространства.

Между тем отсутствие доступа к новым информационным технологиям автоматически превращает слаборазвитые государства всего лишь в потребителей информации, а это, в свою очередь, предопределяет их информационную незащищенность. Такие страны не способны производить конкурентоспособный информационный продукт и вынуждены потреблять зарубежный, что позволяет более сильным соседям использовать эту ситуацию для оказания прямого воздействия на общественное мнение, политические элиты и руководство.

Во многом вследствие этого наиболее развитые государства, которые не принадлежат к так называемому «западному сообществу», активно стремятся противодействовать дальнейшему сохранению цифрового неравенства. Например, в АТР решением этой проблемы занята такая структура, как Азиатско-Тихоокеанский экономический союз (АТЭС), и в частности его рабочая группа по коммуникациям, которая занимается вопросами электронной коммерции [27, c. 76].

Помимо этого, как справедливо отмечает известный белорусский исследователь Ю.И. Малевич, технологические успехи стран АТР, и в первую очередь КНР, в области информационных технологий породили ряд социальных и законодательных противоречий, касающихся информационной безопасности государств. Они связаны прежде всего с обеспечением доступа значительной части населения к средствам массовой коммуникации, который ограничивается на законодательном уровне, так как руководство стран АТР опасается распространения в таких государствах, как КНР, СРВ и КНДР, нежелательной информации [13, c. 216-217].

В определенной степени аналогичная ситуация характерна и для стран Арабского Востока. Такая неправительственная структура, как «RAITNET», включает в себя университеты, исследовательские организации, государственные и частные компании из более чем двадцати стран [27, c. 74]. В целом обстановка в этом регионе оценивается как более благополучная, так как первоначально в ведущих странах региона Ближнего и Среднего Востока население имело больше доступа к средствам массовой информации. Однако сейчас нельзя не заметить, что в последние годы ситуация в отдельных государствах значительно ухудшилась [22].

Исходя из вышесказанного, следует констатировать, что сложившееся в последние десятилетия положение с цифровым неравенством в мировом информационном пространстве вызывает серьезную обеспокоенность во многих странах мира. Не является в данном случае исключением и Российская Федерация [4, c. 3-6].

На протяжении длительного отрезка исторического времени Советский Союз стремился сдерживать информационную войну со стороны западных государств, однако в конечном итоге потерпел поражение. Причины этого поражения требуют отдельного исследования, которое выходит за рамки предмета данной работы.

Тем не менее, следует подчеркнуть, что после распада СССР Российская Федерация сохранила значительную часть технологических мощностей бывшего СССР, использование которых позволяет не только обеспечить безопасность внутреннего информационного пространства России, но и достаточно активно действовать в ближнем и дальнем зарубежье [30]. В противном случае даже бывшие союзные республики весьма скоро могут оказаться за пределами влияния Москвы.

В связи с этим следует согласиться с мыслью о том, что одной из наиболее существенных угроз для будущей российской внешней политики станет постепенное «выдавливание» России из стран ближнего зарубежья, что уже сегодня достаточно очевидно просматривается на примере балтийских республик

Заметное потепление в международных отношениях и демократизация российского общества не исключают сам факт существования геополитической информационно-психологической экспансии. Поэтому политическому руководству России следует признать и необходимость принятия экстренных мер противодействия.

Не менее серьезной проблемой являются так называемые «неадекватные угрозы», связанные, в частности, с деятельностью негосударственных субъектов международной коммуникации, включая ТНК, крупные компании, фирмы и т.д. [23, c. 210-211] К таким, в том числе, относятся криминальные группы хакеров, которые уже сегодня способны нанести урон системе информационной безопасности любого государства и зачастую финансируются заинтересованными экономическими субъектами. Это касается даже США, защита информации в которых требует огромных затрат и организована на самом высоком уровне. Тем не менее, только в 1998 г. хакеры проникли в компьютерную систему НАСА и Агентства информационных систем обороны этой страны [27, c. 90].

В силу этого пересмотр приоритетов и акцентов в оценке проблем национальной безопасности поставили науку и практику перед необходимостью разработки совершенно нового аспекта этой проблемы – безопасности информационной.

С тех пор, как в 1992 г. «информационная безопасность» была нормативно закреплена в качестве самостоятельной составляющей безопасности [Закон Российской Федерации «О безопасности», 5 марта 1992 г. Ст. 13], существенно активизировалась деятельность государства по созданию условий для развития информационной сферы общества и обеспечения ее функционирования в условиях существования угроз различного характера.

К числу безусловно важных событий, произошедших с того времени, следует отнести, во-первых, подписание Президентом Российской Федерации Окинавской хартии глобального информационного общества и, во-вторых, утверждение им Доктрины информационной безопасности.

Подписание Окинавской хартии продемонстрировало совпадение представлений руководства России и других развитых государств об информационно-коммуникационных технологиях как важном факторе формирования общества двадцать первого века. Кроме того, оно выявило политическую волю российского государства не только совместно с другими государствами мира участвовать в формировании постиндустриального общества, создавать условия для глобализации мирового информационного пространства, но и способствовать устранению проблемы «цифрового» неравенства, обеспечению свободы информационного обмена между людьми и безопасности этого процесса [Окинавская хартия глобального информационного общества. 22 июля 2000 г., Окинава. Подписана руководителями восьми развитых стран мира, включая Президента Российской Федерации].

Утверждение Доктрины информационной безопасности [Доктрина информационной безопасности Российской Федерации. Утверждена поручением Президента Российской Федерации от 9 сентября 2000 г. № Пр-1897], развивающей и конкретизирующей положения Концепции национальной безопасности Российской Федерации [Концепция национальной безопасности Российской Федерации. В редакции Указа Президента Российской Федерации от 10 января 2000 г. № 24], закрепило официальную систему взглядов на содержание национальных интересов России в информационной сфере, угроз этим интересам, методы противодействия угрозам и систему обеспечения информационной безопасности. Доктрина создала политическую основу согласования деятельности органов государственной власти по реализации национальных интересов в информационной сфере и защите их от внешних и внутренних угроз. Она наметила направления государственной политики по обеспечению практического участия России в деятельности международного сообщества по достижению целей, намеченных Окинавской хартией.

При этом были учтены проблемы развития российского общества, порожденные как советским периодом его истории, так и периодом продолжающихся социально-экономических и политических преобразований. Реализация национальных интересов в информационной сфере, закрепленных в Доктрине, по существу, будет знаменовать создание материальных, экономических и социальных условий, обеспечивающих устойчивое развитие российского общества и его институтов на базе «информационного» производства, информатизации духовной, политической и социальной сфер общественной жизни, поддержания соответствующего современным международным стандартам правового статуса личности.

К настоящему времени сформирована организационная структура системы обеспечения информационной безопасности. С 1992 г. выявление угроз информационной безопасности и подготовка предложений по противодействию этим угрозам возложена законодательством на Совет Безопасности Российской Федерации. В 1993 г. образована Межведомственная комиссия Совета Безопасности Российской Федерации по информационной безопасности, на которую возложена подготовка предложений Совету Безопасности по выработке и реализации основных направлений политики государства в данной области. С 1996 г. в Комитете по безопасности Государственной Думы Российской Федерации существует подкомитет по информационной безопасности, а также экспертный совет по законодательству в области обеспечения информационной безопасности. Трудно переоценить работу, которую выполняют в этой области федеральные органы исполнительной власти.

Интенсивно развивается правовое регулирование отношений в области обеспечения информационной безопасности. Приняты такие базовые законодательные акты как законы «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», «О связи», «О государственной тайне», первая и вторая части Гражданского кодекса Российской Федерации, новые редакции Уголовного и Уголовно-процессуального кодексов Российской Федерации, целый ряд законов, регулирующих отношения в области средств массовой информации, деятельности федеральных органов исполнительной власти по противодействию угрозам национальным интересам в информационной сфере. Продолжает развиваться индустрия средств защиты информации в информационно-телекоммуникационных системах, сетях связи, автоматизированных системах государственного управления, управления предприятиями и производствами.

Совершенствуется система подготовки кадров высшей квалификации по вопросам обеспечения информационной безопасности. Специальности, по которым осуществляется подготовка специалистов в этой области, выделены в отдельный раздел Перечня направлений подготовки и специальностей высшего профессионального образования [Перечень направлений подготовки и специальностей высшего профессионального образования. Утвержден Приказом Министра образования Российской Федерации от 2 марта 2000 г. № 686]. Успешно работает Учебно-методическое объединение вузов по образованию в области информационной безопасности. На начало 2002 г. оно объединяло более 60 высших учебных заведений, которые готовят специалистов, прежде всего, по техническим аспектам обеспечения информационной безопасности. Разворачивается подготовка кадров по ее гуманитарным аспектам.

Большая работа проделана по разъяснению важности создания международной системы обеспечения информационной безопасности. Все большее число государств начинает осознавать наличие в этой области значительных общих интересов, необходимость объединения усилий международного сообщества в борьбе с угрозами, возникающими в информационной сфере. Генеральная Ассамблея Организации Объединенных Наций, начиная с 1998 г., ежегодно принимает резолюции по вопросу «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности».

В этих резолюциях все более отчетливо проявляется озабоченность тем, что информационные технологии могут негативно воздействовать на безопасность государств применительно как к гражданской, так и к военной сферам, и содержится призыв к государствам-членам Организации Объединенных Наций содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также возможных мер по нейтрализации этих угроз.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, являющейся важным фактором общественной жизни, во многом определяющим перспективы успешного осуществления социально-политических и экономических преобразований. В центре этого находятся следующие обстоятельства.

Прежде всего в условиях реализации конституционных прав граждан на свободу экономической, информационной и интеллектуальной деятельности существенно расширяются потребности социально активной части общества в расширении информационного взаимодействия как внутри страны, так и с внешним миром. Это красноречиво характеризуется данными ЮНЕСКО по числу пользователей самими распространёнными видами связи: мобильной и Интернет. Так, в РФ число зарегистрированных пользователей Интернет на начало 2000 г. составляло около 2 млн. человек, а число активно использующих эту сеть — 1,2 млн. человек и продолжает увеличиваться (число пользователей сети Интернет в мире уже достигло 100 млн. человек); в развитых странах каждый десятый человек обеспечен сотовой связью.

Интенсивное развитие информационной инфраструктуры и, прежде всего, информационно-телекоммуникационных систем, средств и систем связи, интеграция в мировое информационное пространство, а также информатизация практически всех сторон общественной жизни, деятельности органов государственной власти и управления существенно усилили зависимость эффективности функционирования общества и государств от состояния информационной сферы. К приведённым выше данным здесь можно добавить, например, позитивные тенденции, характеризующие развитие в России такой чувствительной к новым технологиям сферы, как «электронная» экономика и «электронная» торговля. В России в настоящее время уже существуют десятки Интернет-магазинов, услугами которых активно пользуются около 20% пользователей Сети и их количество постоянно увеличивается (мировой же оборот «электронной» торговли оценивается в несколько млрд. долларов в год и ожидается, что в 21 веке её ежегодный объем будет составлять сотни млрд. долларов).

Общепризнанно, что индустрия информатизации, телекоммуникации и связи, информационных услуг на современном этапе развития человечества является одной из наиболее динамично развивающихся сфер мировой экономики, способной конкурировать по доходности с топливно-энергетическим комплексом, автомобилестроением, производством сельскохозяйственной продукции и определяющей наукоемкость промышленной продукции, ее конкурентоспособность на мировом рынке. Так, только объемы реализации средств вычислительной техники и информатики оценивается более, чем в 1,5 млрд. долларов в год, а с учётом продаж программного продукта — около 4,5 млрд. долларов, что составляет около 5% годового ВВП России (объем современного мирового рынка информационных услуг и технологий по данным ЮНЕСКО приближается к 2 трлн. долл. и составляет уже 15% мировой торговли).

Вместе с тем, приходится отмечать, что информационная инфраструктура, информационные ресурсы во все большей степени становятся ареной межгосударственной борьбы за мировое лидерство, достижение противоборствующими сторонами определенных стратегических и тактических политических целей. Индивидуальное, групповое и массовое сознание людей все в большей степени зависят от деятельности средств массовой информации и массовой коммуникации. К сожалению уже вошли в обиход, в том числе и в международных отношениях, такие понятия, как «информационная война», «информационное противодействие», «информационная операция» и т. п.

Все эти обстоятельства, а также возрастание зависимости российского общества от устойчивого функционирования информационной инфраструктуры делают достижение и обеспечение безопасности национальных интересов Российской Федерации в информационной сфере важным фактором национальной безопасности страны в целом.

Содержание национальных интересов Российской Федерации в информационной сфере закреплено в утвержденной в июне 2006 г. Президентом РФ Доктрине информационной безопасности Российской Федерации. Эти национальные интересы, как уже было сказано выше, включают:

соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;

информационное обеспечение государственной политики Российской Федерации;

развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;

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

По существу, речь идет о создании условий для формирования в России основ информационного общества — общества XXI века.

При этом под информационным обществом мы понимаем такое общество, которое позволяет людям на базе интенсивного развития «информационной» экономики и эффективного использования интеллектуальных ресурсов раскрыть потенциальные возможности и реализовать свои чаяния как отдельным личностям, так и обществу в целом.

В политическом плане данная задача поставлена Президентом Российской Федерации, подписавшим от имени государства Окинавскую хартию глобального информационного общества. В Хартии, в частности, закреплено, что главы подписавших ее государств «подтверждают приверженность принципу участия в этом процессе: все люди повсеместно, без исключения должны иметь возможность пользоваться преимуществами глобального информационного общества».

Представляется, что полномасштабное участие России в формировании глобального информационного общества, может рассматриваться как одна из стратегических задач обеспечения ее национальной безопасности, решение которой будет осуществляться в условиях преодоления реально существующих и могущих возникнуть трудностей и потребует определенного времени, а также соответствующей поддержки со стороны государства.

Если вернуться к рассмотрению российских национальных интересов в информационной сфере, сформулированных в Доктрине информационной безопасности, то для реализации той группы интересов, которые связаны с соблюдением конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечением духовного обновления России, сохранением и укреплением нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны, в первую очередь требуется повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа РФ, что само по себе представляет теперь непростую задачу. Ведь не секрет, что в условиях раскола общества на «бедных» и «богатых» весьма сложно обеспечить равные возможности пользования передовыми информационными технологиями для всех членов общества. Поэтому государство должно предусматривать создание и развитие соответствующих социальных институтов поддержки в этих вопросах определенной части населения.

Необходимо далее совершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации и одновременно обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

И наоборот, право свободного доступа к информации не должно вести к нарушению конституционного права человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени. К сожалению, примеров нарушения этого столь много и они настолько на слуху, что особо останавливаться на них нет необходимости.

Необходимо также гарантировать свободу массовой информации, запрет цензуры и одновременно укреплять механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации.

Успешному решению этих задач препятствуют факторы и обстоятельства, которые Доктриной информационной безопасности отнесены к разряду «угроз». Основными из них являются:

принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем. Это на первый взгляд может показаться не столь актуальным, но развернувшаяся в последнее время острая конкурентная борьба в области телевещания, одного из наиболее «мощных» сегментов СМИ, свидетельствует о том, что сбрасывать со счетов эту угрозу сейчас нельзя;

противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на охрану личной и семейной тайны, тайны переписки, телефонных переговоров и иных сообщений. По данным МВД России за последние три года количество зафиксированных фактов преступлений, предусмотренных статьей 138 УК Российской Федерации «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» возросло в 75 раз;

нерациональное, чрезмерное закрытие общественно необходимой информации. Все мы знаем, какие тяжелые последствия имело сокрытие информации о реальных масштабах аварии на Чернобыльской АЭС. И хотя грань здесь подчас весьма тонкая и трудно оценить, где потери для общества больше: в случае полного или частичного закрытия информации или, наоборот, в случае безусловного доступа общественности к разнородной, нередко противоречивой информации о чрезвычайных происшествиях, действующим законодательством соответствующие границы закрытия определены и его следует выполнять.

Угрозами также являются:

противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание. На наш взгляд эта сфера пока недостаточно разработана, и в том, что по ней публикуется, немало антинаучного, а подчас и просто шарлатанства;

дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы. В определенной мере это вызвано тем, что значительное число документов, в том числе кино-, фото-, видеодокументов хранится вне государственных архивов, а решение задачи обеспечения сохранности документов далеко не всегда оказывается посильным для их создателей. Основная причина такого положения заключается в отсутствии правовых актов федерального уровня, касающихся деятельности средств массовой информации в части вопросов сохранности, отбора и передачи аудиовизуальных документов на постоянное хранение в государственные архивы [10].

Весьма негативной для национальных интересов России является тенденция вытеснения российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур. По данным МПТР по состоянию на прошлый год на территории России зарегистрированы 38 электронных и 66 печатных СМИ, созданных с привлечением иностранных инвестиций или в числе учредителей которых состоят иностранные юридические лица. 1157 иностранных изданий получили разрешение на распространение своей продукции в нашей стране. И хотя в целом у российского руководства конструктивная позиция в отношении такой ситуации надо ясно осознавать, что это одновременно создает жесткие условия российским производителям в информационной сфере [23].

В этой же группе угроз находятся:

девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе. Эта угроза практически ежедневно, ежечасно реализуется на нашем телевидении и в каком-либо дополнительном обосновании своей реальности не нуждается;

снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных.

Следующая группа национальных интересов России связанна с информационным обеспечением государственной политики Российской Федерации. Для их достижения требуется:

во-первых, интенсифицировать формирование государственных отрытых информационных ресурсов, повысить эффективность их хозяйственного использования;

во-вторых, укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских граждан, граждан зарубежных государств. Надо сказать, что эта вполне понятная с позиции государства задача была неправильно понята рядом негосударственных СМИ, воспринявших её как их дискриминацию. Вместе с тем, во-первых, ничего нет естественнее того факта, что собственник заботится о своей собственности, а во-вторых, никто не собирается ущемлять права негосударственных СМИ, предусмотренных действующим законодательством о СМИ [23].

Основные угрозы в этой области заключаются в следующем.

Во-первых, это монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами, по ряду причин не заинтересованными в объективном освещении государственной политики Российской Федерации;

Во-вторых, это блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории. Характерным примером здесь могут служить трудности, с которыми пришлось столкнуться, в частности, российскому МИДу при попытках разъяснения политики России в Чечне, когда замалчивалась официальная информация о событиях на Кавказе, и, наоборот, распространялась неофициальная непроверенная, а подчас и ложная информация, в частности, размещаемая на «чеченских» сайтах в Интернете.

Наконец, угрозой является низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров в этой области, отсутствия эффективной системы формирования и реализации государственной информационной политики.

Третья группа национальных интересов связана с развитием современных информационных технологий, российской индустрии информации, обеспечением потребностей внутреннего рынка ее продукцией и выхода этой продукции на мировой рынок, а также с обеспечением накопления, сохранности и эффективного использования отечественных информационных ресурсов. Для этого требуется развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации. В настоящее время наблюдается, если так можно выразится, «разорванность» национального информационного пространства, что особенно опасно по отношению к таким регионам, как Дальний восток и Калининград, находящимися в непосредственном соседстве с экономически и информационно сильными соседями. Это подтверждается, в частности, тем, что центральные СМИ вспоминают о регионах, только если там случается какой-нибудь скандал, а местные СМИ не в состоянии полно отразить происходящее в центре. Об этом , в частности, говорил Президент Российской Федерации В.В.Путин на встрече в Кремле с главными редакторами российских СМИ [23].

Необходимо развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов. В настоящее время в стране насчитывается более 300 тысяч различных баз данных (только официально зарегистрированных около 6,5 тысяч), часто дублирующих друг друга, созданных в разных форматах, не стыкующихся между собой, что, конечно, не способствует эффективному использованию затрачиваемых на создание таких баз средств.

Важной задачей является развитие в Российской Федерации производства конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширение участия России в международной кооперации производителей этих средств и систем. Министерством связи России и другими заинтересованными структурами прилагаются немалые усилия по решению этого вопроса, но конкуренция в этом секторе экономики слишком высока, а российское отставание в элементной базе и ограниченность финансовых средств пока не позволяют добиться необходимых успехов. Поэтому очень важно обеспечить государственную поддержку российских фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Основной угрозой национальным интересам России в этой области являются противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий [10].

Сплошь и рядом при заключении договоров в этой области российским партнёрам предлагаются условия, не позволяющие в полной мере реализовывать интересы государства. Большой урон российской промышленности наносит практика закупки органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих или почти не уступающих по своим характеристикам зарубежным образцам. Не всегда, по-видимому, такие решения принимаются на бескорыстной основе. В результате происходит вытеснение с рынка России собственных производителей средств информатизации, телекоммуникации и связи. Особо чувствительный урон промышленности наносит большой отток за рубеж специалистов и правообладателей интеллектуальной собственности.

Наконец, последняя сформулированная в Доктрине информационной безопасности группа национальных интересов связана с защитой информационных ресурсов от несанкционированного доступа, обеспечением безопасности информационных и телекоммуникационных систем.

Для достижения этого требуется повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами. Надо сказать, что благодаря твёрдой позиции ряда ведомств, прежде всего, Министерства обороны, ФСБ, ФАПСИ, Гостехкомиссии, ситуация в большинстве своём выглядит стабильной.

Однако и здесь, ввиду хронического недофинансирования в последнее время этой сферы экономики Россия нуждается в интенсификации развития отечественного производства аппаратных и программных средств защиты информации. Важной и актуальной является задача расширения международного сотрудничества Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

К числу основных угроз данной составляющей национальных интересов следует отнести деятельность иностранных разведок и (чего не было так развито раньше) криминальных элементов по:

противоправному сбору и использованию информации;

внедрению в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

разработке и распространению программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

перехвату информации по техническим каналам.

Этот тип угроз условно можно отнести к внешним [10].

Другой тип угроз внутреннего характера связан с нарушением обслуживающим персоналом технологии обработки информации; с использованием несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры; с нарушением законных ограничений на распространение информации.

Решение перечисленных задач и противодействие выделенным угрозам предполагает необходимость дальнейшего совершенствования нормативного правового обеспечения информационной безопасности. В этой связи под эгидой Совета Безопасности Российской Федерации подготовлен проект Концепции нормативного правового обеспечения информационной безопасности Российской Федерации. Концепция призвана создать методологическую основу для согласованной деятельности всех субъектов законодательной инициативы в сфере совершенствования правового обеспечения информационной безопасности.

**Глава 2. Политико-правовые основы обеспечения информационной безопасности РФ**

Основным направлением противодействия информационной экспансии геополитических соперников России и «неадекватных угроз» со стороны криминальных группировок является создание информационно-психологических структур для обеспечения психологической безопасности личности, общества, государства.

Их конструктивная задача – разработка и осуществление стратегических и оперативных мер по предупреждению и нейтрализации негативных информационно-психологических воздействий на федеральном, региональном и местном уровнях.

Такая деятельность стала активно проводиться лишь со второй половины 1990-х годов, когда Российская Федерация столкнулась с целой серией разнообразных угроз в информационной сфере, справиться с которыми обычными мерами оказалось невозможным. Помимо этого, все более существенно начало сказываться технологическое отставание России от западных государств, которое явилось последствием разрушения российского военно-промышленного комплекса в начале 1990-х годов. Как подчеркивает А.А. Чернов, в этот момент у развитых государств появился соблазн использовать имеющиеся у них преимущества в компьютерных технологиях и средствах информационно-психологического воздействия на индивидуальное и общественное сознание для информационной, политической, экономической и культурной экспансии [27, c. 92].

Ответом стала принципиально новая политика российского руководства, напрямую связанная с приходом на пост главы российского правительства так называемых «силовиков»: Е. Примакова, С. Степашина и, наконец, В. Путина, которые не только высказывались за восстановление сильного российского государства, но начали принимать конкретные меры по реализации этой задачи.

В рамках новой политики с целью сокращения разрыва между Российской Федерацией и развитыми странами по уровню распространения, производства и эффективности использования информационных продуктов и технологий был разработан и принят целый ряд основополагающих документов, которые регулируют различные направления государственной информационной политики Российской Федерации.

Именно эти документы определяют основы информационной деятельности российских правительственных структур и средств массовой и сетевой информации. К ним, в частности, относятся:

1. Концепция государственной информационной политики РФ, которая была разработана в 1998 г, одобрена Комитетом по информационной политике и связи Государственной Думы Федерального Собрания 15 октября 1998 г. и Постоянной палатой по государственной политике Политического консультативного совета при Президенте Российской Федерации 21 декабря 1998 г., опубликована в 1999 г. и разослана во все органы государственной власти на федеральном уровне и уровне субъектов Федерации [2, c. 17-19].

В этом документе были провозглашены следующие принципы государственной политики в сфере информации:

принцип открытости – все основные мероприятия информационной политики открыто обсуждаются обществом, и государство учитывает общественное мнение;

принцип равенства интересов – политика в равной степени учитывает интересы всех участников информационной деятельности, вне зависимости от их положения в обществе, формы собственности и гражданства;

принцип системности – при реализации тех или иных решений должны учитываться их последствия при состоянии всех объектов и субъектов, затрагиваемых этими решениями;

принцип приоритетности производителя – при равных условиях приоритет отдается конкурентоспособному отечественному производителю информационно-коммуникационных средств, продуктов и услуг;

принцип социальной ориентации – основные мероприятия государственной информационной политики должны быть направлены на обеспечение социальных интересов общества;

принцип государственной поддержки – мероприятия информационной политики, направленные на информационное развитие социальной сферы, финансируются преимущественно государством;

принцип приоритетности права – развитие и применение правовых методов имеет приоритет перед экономическими и административными решениями проблем.

Анализируя основные принципы государственной информационной политики Российской Федерации, следует отметить, что нынешнее российское руководство активно стремится централизовать государственную политику в информационной сфере, что позволяет решить сразу две задачи, которые относятся к области внешней политики.

Во-первых, это контроль над распространением информации внутри российского информационного пространства и противодействие попыткам других стран и негосударственных субъектов массовой коммуникации взять его под собственный контроль.

Во-вторых, речь идет о последовательной и целенаправленной стратегии по усилению российского информационного присутствия за рубежом. Это достижимо только при условии государственной координации и поддержки информационной политики, а также в случае соответствия ее целей внутри и за пределами страны.

2. Концепция формирования информационного общества в России была одобрена 28 мая 1999 г. Государственной комиссией по информатизации при Государственном комитете Российской Федерации по связям и информатизации [27, c. 100].

В этом документе изложены основные предпосылки перехода России к информационному обществу, а также характерные особенности этого процесса для Российской Федерации и основные направления деятельности российских правительственных структур по реализации этой концепции.

С точки зрения внешней политики РФ, по мнению автора, особый интерес представляют положения, которые касаются места и роли российского государства в переходном процессе. В качестве одной из важнейших составляющих этого перехода указывается участие Российской Федерации в процессе международного информационного обмена, в соответствии с одноименным федеральным законом [11, c. 3-11].

Вместе с тем, обе вышеуказанные концепции касаются, в первую очередь, такого аспекта российской информационной политики, как участие России в формировании глобального информационного общества, которое включает в себя следующие элементы: взаимодействие с другими государствами, обмен информационными технологиями и продукцией, участие в деятельности международных и региональных структур, которые содействуют этому процессу.

Необходимо отметить, что активное участие России в таком международном сотрудничестве, несомненно, является частью внешней политики российского государства. При этом речь идет именно об одном из направлений внешнеполитического курса, так как оба рассмотренных документа являются обязательными для исполнения.

К началу 2000-х годов в России была создана международно-правовая база для сотрудничества с другими странами в области информационных технологий, их защиты, безопасного распространения и использования. Однако более важной задачей для Российской Федерации явилось обеспечение собственной информационной безопасности, что позволило этой стране претендовать на роль не только потребителя, а производителя информации, а также эффективно противостоять экспансии со стороны других государств и потенциальным рискам и угрозам.

Исходя из этого, по мнению автора, важнейшим документом в сфере информационной политики, который был принят в России и реализуется в настоящее время, является Доктрина информационной безопасности 2000 г.

Доктрина информационной безопасности Российской Федерации является базовым концептуальным документом, который определяет основные направления обеспечения одного из ключевых направлений безопасности российского государства. Она была одобрена Советом Безопасности РФ 23 июня и утверждена президентом России В. Путиным 9 сентября 2000 г. В доктрине отмечается, что современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Как верно отмечает белорусский исследователь С.А. Трахименок, информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности любого государства [21, c. 37]. Национальная безопасность Российской Федерации также существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать, учитывая, в частности, усиливающиеся угрозы со стороны криминальных группировок, террористов, приверженцев любой экстремальной идеи и других деструктивных общественных сил [24, c. 112].

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [10, c. 158-159].

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности. Решение этой проблемы является первостепенным для дальнейшей разработки доктринальных основ обеспечения информационной безопасности [21, c. 64-65].

В этом документе закреплены четыре составляющие национальных интересов Российской Федерации в информационной сфере. Первая составляющая включает в себя соблюдение конституционных прав и свобод человека и гражданина области получения информации и ее использования, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Второй составляющей является информационное обеспечение государственной политики Российской Федерации, которое заключается в доведении до сведения российской и мировой общественности достоверной и позитивной информации о государственной политике России, ее официальной позиции по социально значимым вопросам российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Именно эта составляющая информационной безопасности российского государства имеет самое непосредственное отношение к области внешней политики и отражает важнейшие внешнеполитические задачи Российской Федерации на международной арене.

Для достижения этих целей создатели доктрины предлагают следующие меры:

Укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;

Интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования [10, c. 158-159].

По мнению автора, эти меры носят достаточно половинчатый характер, так как Российская Федерация обладает сегодня развитой системой печатных, электронных и сетевых средств массовой информации. Проблема заключается скорее в низкой эффективности информационной продукции, которая предлагается жителям других государств. Зачастую российские масс-медиа открыто вмешиваются во внутриполитические процессы на территории других государств, что вызывает негативную реакцию местного населения, т.е. обратный эффект. При этом необходимо отметить, что воздействие на общественное мнение с целью формирования устойчивых политических настроений является сегодня сложнейшим процессом, требующим приложения значительных информационных ресурсов, прогнозирования и объективной оценки результатов [25, c. 199-200].

Третьей составляющей в доктрине названо развитие новых информационно-коммуникационных технологий, в том числе в области индустрии средств информатизации, телекоммуникации и связи, а также обеспечение потребностей внутреннего рынка ее продукцией и выход на мировой рынок.

Эта составляющая национальных интересов Российской Федерации в информационной сфере включает в себя также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Для достижения этого предлагается развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации; развивать индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов; развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем; обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи [10, c. 158-159].

Еще одна составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории РФ. Среди мер, которые предлагается осуществить для реализации этой задачи, называются такие, как повышение безопасности информационных систем, включая сети связи; обеспечение защиты сведений, которые оставляют государственную тайну; расширение международного сотрудничества Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере и т.д. [10, c. 163]

Особый интерес при анализе текста доктрины представляют виды угрозы информационной безопасности Российской Федерации, которые перечислены в разделе 2.

Следует отметить, что изучение этого перечня позволяет соотнести риски и угрозы, стоящие сегодня перед российским государством, с аналогичными явлениями, с которыми сталкивается в настоящее время Республика Беларусь.

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 [10, c. 162-163].

Среди вышеперечисленных угроз к сфере внешней информационной безопасности можно отнести следующие.

Из первой группы (угрозы конституционным правам и свободам человека и гражданина): вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур; девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях противоречащих ценностям, принятым в российском обществе; манипулирование информацией (дезинформация, сокрытие или искажение информации), в т.ч. и извне [10, c. 165].

Из второй группы (угрозы информационному обеспечению государственной политики РФ): монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами; блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории [10, c. 164-165].

Из третьей группы (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): противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий; закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам; вытеснение с рынка российских производителей средств информатизации, телекоммуникации и связи; увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности [10, c. 166].

Из четвертой группы (угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России): уничтожение, повреждение, разрушение или хищение машинных и других носителей информации; перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации; использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры; несанкционированный доступ к информации, находящейся в банках и базах данных; нарушение законных ограничений на распространение информации и т.д. [10, c. 167].

Помимо этого, в доктрине указаны источники угроз информационной безопасности России, среди которых необходимо выделить те из них, которые касаются внешней безопасности.

В соответствии с этим документом источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние, хотя, по мнению автора, между ними существует тесная взаимосвязь. В отдельных случаях внутренние источники могут квалифицироваться как внешние, и наоборот.

К внешним источникам доктрина относит:

деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов России в информационной сфере;

стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

обострение международной конкуренции за обладание информационными технологиями и ресурсами;

деятельность международных террористических организаций;

увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним [10, c. 167-168].

К внутренним источникам, которые при определенных обстоятельствах могут быть рассмотрены как внешние, относятся: критическое состояние отечественных отраслей промышленности; недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации; недостаточная экономическая мощь государства; недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности; отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти и различных отраслей экономики и социальной сферы и т.д.

В доктрине также перечислены меры, которые уже были предприняты федеральными, региональными и местными властями на протяжении 1990-х годов для улучшения ситуации в сфере обеспечения информационной безопасности России. К таким мерам относятся:

Начало формирования базы правового обеспечения информационной безопасности, а именно принятие федеральных законов и работа по созданию механизмов их реализации;

Мероприятия по обеспечению информационной безопасности различных уровней власти;

Укрепление государственной системы защиты информации [10, c. 170].

Вместе с тем, как утверждается в доктрине, анализ состояния информационной безопасности Российской Федерации показывает, что ее уровень не в полной мере соответствует потребностям общества и государства. Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение. Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере приводят к серьезным негативным последствиям. Недостаточна также государственная поддержка деятельности российских информационных агентств по продвижению их продукции на зарубежный информационный рынок. Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов.

Помимо этого, отставание отечественных информационных технологий вынуждает федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации и органы местного самоуправления при создании информационных систем идти по пути закупок импортной техники и привлечения иностранных фирм, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения [10, c. 172-173].

В доктрине утверждается, что сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательного решения таких задач, как (автором указаны те, которые касаются сферы обороны, безопасности и внешней политики):

разработка основных направлений государственной политики в области обеспечения информационной безопасности РФ, а также мероприятий и механизмов, связанных с реализацией этой политики;

развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Российской Федерации, а также системы противодействия этим угрозам;

разработка федеральных целевых программ обеспечения информационной безопасности РФ;

разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации, а также сертификации этих систем и средств;

развитие научно-практических основ обеспечения информационной безопасности Российской Федерации с учетом современной геополитической ситуации, условий политического и социально-экономического развития России и реальности применения «информационного оружия»;

разработка методов повышения эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;

обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность;

разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономическими важными производствами;

развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;

создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;

расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;

обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;

создание единой системы подготовки кадров в области информационной безопасности и информационных технологий и т.д. [10, c. 173-175].

Исходя из анализа вышеперечисленных пунктов, следует отметить, что на сегодняшний день российское руководство проводит целенаправленную политику по укреплению и расширению информационного обеспечения национальной обороны, безопасности, внешней политики. При этом правительство Российской Федерации не только ставит задачи, но предлагает конкретные методы их решения, которые подразделяются на общие и специальные.

Общие методы, в свою очередь, делятся на правовые, организационно-технические и экономические. Ниже указаны те из них, которые относятся к правовой сфере и касаются сфер обороны, безопасности и внешней политики. Среди организационно-технических и экономических методов, по мнению автора, указаны прикладные методики обеспечения безопасности деятельности различных технических объектов и экономических субъектов разных форм собственности.

К правовым же методам, в частности, относятся уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России; законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи; определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций [10, c. 176].

К специальным методам относятся конкретные подходы к обеспечению информационной безопасности в таких сферах как экономика, внутренняя политика, внешняя политика, наука и техника, духовная сфера, общегосударственные информационные и телекоммуникационные системы, оборона, правоохранительная и судебная системы.

При этом необходимо вновь обратить внимание на тесную взаимосвязь между угрозами в сфере внутренней и внешней политики:

К внутриполитическим угрозам, которые непосредственно относятся к сфере международной политики, можно причислить такие как:

Распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;

Деятельность общественных объединений, направленная на насильственное изменение конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации [10, c. 182].

Примечательно, что в обоих случаях не указывается, идет ли речь о российских или зарубежных структурах, однако очевидно, что такие организации стремятся оказать воздействие на общественное мнение Российской Федерации с целью склонить ее население к тому или иному политическому выбору. По этой причине необходимо еще раз подчеркнуть особую роль средств массовой информации, которые должны учитывать фактор информационной безопасности в своей деятельности [5, c. 21].

Внешнеполитическими угрозами, по мнению разработчиков доктрины, для России являются:

Информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;

Распространение за рубежом дезинформации о внешней политике РФ;

Нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;

Попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом, представительств РФ при международных организациях.

Помимо этого, в отдельную группу выделены так называемые внутренние угрозы информационной безопасности России в сфере внешней политики, к числу которых относятся:

Нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику Российской Федерации, и на подведомственных им предприятиях, в учреждениях и организациях;

Информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности Российской Федерации;

Недостаточную информированность населения о внешнеполитической деятельности России [10, c. 184].

Для решения этих проблем авторы доктрины предлагают:

Разработать основные направления государственной политики в области совершенствования информационного обеспечения внешнеполитического курса Российской Федерации;

Разработать и реализовать комплекс мер по усилению информационной безопасности информационной инфраструктуры федеральных органов исполнительной власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом, представительств России при международных организациях;

Создать российским представительствам и организациям за рубежом условия для работы по нейтрализации распространяемой там дезинформации о внешней политике Российской Федерации;

Совершенствовать информационное обеспечение работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом;

Совершенствовать информационное обеспечение субъектов РФ по вопросам внешнеполитической деятельности, которые входят в их компетенцию [10, c. 184-185].

В этом контексте крайне важным является обеспечить свободный доступ граждан Российской Федерации к любой информации, которая имеет открытый характер и способна содействовать развитию полноценной и гармоничной личности. Это право можно с полной уверенностью оценивать в качестве основополагающего элемента современной концепции прав человека и гражданина [16, c. 65].

В сфере науки и техники внешними угрозами являются:

стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах;

создание льготных условий на российском рынке для иностранной научно-технической продукции и стремление развитых стран в то же время ограничить развитие научно-технического потенциала России (скупка акций передовых предприятий с их последующим перепрофилированием, сохранение экспортно-импортных ограничение и т.д.);

политику западных стран, направленную на дальнейшее разрушение унаследованного от СССР единого научно-технического пространства государств – участников СНГ за счет переориентации на западные страны их научно-технических связей, а также отдельных, наиболее перспективных научных коллективов;

активизацию деятельности иностранных государственных и коммерческих предприятий, учреждений и организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб [10, c. 185-186].

В качестве внутренних угроз в этой сфере безопасности названы такие, как резкое снижение финансирования научных учреждений, утечка за рубеж идей и технологий, технологическое отставание России от западных стран в сфере информационных технологий, что вынуждает российских производителей импортировать зарубежные комплектующие и программное обеспечение, проблемы с патентной защитой российских изобретений и т.д.

Реальный путь противодействия угрозам информационной безопасности РФ в области науки и техники – это, по мнению авторов доктрины, совершенствование законодательства Российской Федерации, регулирующего отношения в данной области, и механизмов его реализации.

В этих целях государство должно способствовать созданию системы оценки возможного ущерба от реализации угроз наиболее важным объектам обеспечения информационной безопасности Российской Федерации в области науки и техники, включая общественные научные советы и организации независимой экспертизы, вырабатывающие рекомендации для федеральных органов государственной власти и органов государственной власти субъектов РФ по предотвращению противоправного или неэффективного использования интеллектуального потенциала России.

В духовной сфере в качестве угроз определяются: неконтролируемое расширение сектора зарубежных масс-медиа в российском информационном пространстве, использование зарубежными специальными службами средств массовой информации, действующих на территории России, для нанесения ущерба обороноспособности страны и безопасности государства, распространения дезинформации, вытеснения русского языка в большинстве постсоветских государств и т.д. [1, c. 8-9].

В ответ составители доктрины предлагают заняться духовно-нравственным воспитанием подрастающего поколения и содействовать укреплению патриотизма [10, c. 188-189].

В общегосударственных информационных и телекоммуникационных системах в качестве основной внешней угрозы рассматривается деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля над функционированием информационных и телекоммуникационных систем. Естественной защитной мерой называется усиление защиты информации.

И, наконец, угрозами в сфере обороны для современной России 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 РФ в сфере обороны [10, c. 193].

Помимо этого, в качестве внутренних угроз для обороноспособности Российской Федерации указаны такие факторы как возможная подрывная информационно-пропагандистская деятельность, подрывающая престиж Вооруженных Сил РФ и их боеготовность, а также нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов.

Для преодоления этих проблемы предлагается систематически выявлять потенциальные угрозы и их источники, структурировать цели обеспечения информационной безопасности в области обороны и определять соответствующие практические задачи; осуществлять защиту информации, которая имеет военное значение, а также более активно применять специфические армейские методы защиты (маскировка, разведка, радиоэлектронная борьба и т.д.).

В целом противодействие информационным угрозам в сфере обороны является одной из наиболее сложных и многофакторных задач по обеспечению национальной безопасности, так как подразумевает целый комплекс психолого-идеологических мероприятий, направленных на сохранение боеспособности вооруженных сил государств и иных силовых структур в мирное и военное время [12, c. 64-69].

Разведывательная деятельность специальных служб иностранных государств, а также международных преступных сообществ, организаций и групп, связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел рассматривается также в качестве первостепенной угрозы для объектов обеспечения информационной безопасности в правоохранительной и судебной сферах.

Еще одной внешней угрозой является деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов. В данном случае также предлагается обеспечить высочайший уровень защиты конфиденциальной информации и повышать уровень подготовки соответствующих специалистов [10, c. 195-197].

Необходимо также отметить, что особое значение в процессе обеспечения информационной безопасности придается международному сотрудничеству в этой сфере. Такое взаимодействие Российской Федерации с другими государствами заявлено как неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое сообщество. Это сотрудничество должно, по мнению разработчиков доктрины, способствовать повышению информационной безопасности всех членов мирового сообщества, включая Российскую Федерацию [10, c. 198].

Основными направлениями международного сотрудничества Российской Федерации в этой области являются:

запрещение разработки, распространения и применения так называемого «информационного оружия»;

обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;

координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;

предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организационной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

При этом авторы доктрины подчеркивают необходимость интенсивного взаимодействия России с другими странами СНГ [10, c. 199]. Исходя из этого, необходимо еще раз обратить внимание на важность детального анализа и заимствования отдельных положений российской доктрины в ходе разработки нормативно-правовой базы обеспечения информационной безопасности Республики Беларусь.

Помимо этого, представляется необходимым как в нашей стране, так и в России в рамках дальнейшей разработки документов, регламентирующих защиту информационных интересов обеих стран рассмотреть необходимость присутствия в концептуальных документах такой важной составляющей как совместные действия по обеспечению информационной безопасности Союзного Государства Беларуси и России [3, c. 12-13].

К настоящему времени созданы все условия для обеспечения информационной безопасности Российской Федерации, которое подразумевает всестороннее противодействие имеющимся рискам и угрозам на основании принятой в начале 2000-х годов и действующей в настоящее время политико-правовой основы для этой деятельности.

Таким образом, осуществленный в данной главе анализ Доктрины информационной безопасности Российской Федерации позволяет сделать следующие выводы:

Во-первых, принятая в 2000 г. доктрина представляет собой основополагающий документ, который не только определяет сущность и содержание информационной безопасности такого значимого субъекта международных отношений, как Россия, но и достаточно подробно описывает отдельные ее составляющие, исходя из современных условий социально-политического, экономического и духовно-гуманитарного развития российского государства.

Во-вторых, доктрина явилась нормативно-правовой основой для дальнейшей деятельности российского разведывательного сообщества, правоохранительной судебной системы, позволив не только определить и классифицировать угрозы и риски для информационной безопасности Российской Федерации, но предоставив возможность разработать комплекс мер, направленных на их предотвращение таких угроз. Особое внимание заслуживает детальное рассмотрение специфических рисков, которые характерны для отдельных направлений государственной политики, и выявление наиболее эффективных методов борьбы с ними.

В-третьих, российская доктрина может стать моделью для разработки, принятия и практической реализации аналогичных нормативно-правовых актов в других постсоветских странах, особенно учитывая то обстоятельство, что Россия как великая держава сталкивается с несравнимо большим объемом рисков и угроз, чем средние и малые государства. Помимо этого, анализируя содержание доктрины и пытаясь адаптировать его к белорусским условиям, следует обратить внимание на различный потенциал специальных и разведывательных служб Республики Беларусь и Российской Федерации.

Аналогичное утверждение может в полной мере относиться и к структурам правоохранительной и судебной системы обеих стран. По этой причине, заимствуя российский опыт, необходимо внимательно сопоставлять возможности обоих государств и детально проанализировать стоящие перед белорусскими и российскими исполнительными и судебными структурами цели и задачи.

**Заключение**

Проведенный в данной работе анализ обеспечения информационной безопасности Российской Федерации позволяет сделать вывод, что именно это направление государственной политики России является на сегодняшний момент одним из приоритетных элементов внешнеполитической стратегии российского государства. Поскольку эффективность информационной безопасности в значительной степени определяет место и роль любого государства в мировой политике, то правительство России начало уделять особое внимание реализации этой задачи в первой половине 2000-х годов. В этот период российская внешняя политика претерпела наиболее значимые изменения, вызванные постепенным преобразованием постсоветского пространства под усиливающимся контролем других влиятельных субъектов международных отношений.

В этих условиях Российская Федерация предприняла ряд усилий, направленных на укрепление присутствия в мировом информационном пространстве. Анализ этих действий, проведенный в данной работе, позволяет сделать следующие выводы.

Во-первых, государственная информационная политика России нацелена в настоящее время на формирование и поддержание благоприятного имиджа российского государства. С этой целью используется деятельность структур внешнеполитического и внешнеэкономического аппарата (дипломатических и консульских представительств, информационных центров, торговых домов и т.д.), которые не только выполняют свои прямые обязанности, но и обязаны пропагандировать российские традиции и культурные ценности.

Не менее существенной задачей для современной российской дипломатии является поддержка использования русского языка в странах ближнего и дальнего зарубежья, а также помощь в изучении российской истории в различных государствах.

При этом следует подчеркнуть, что на сегодняшний день осуществление этих задач наталкивается на целый ряд проблем, связанных, в первую очередь, с недостатком финансирования государственной информационной политики Российской Федерации за рубежом. Еще одной проблемой является недостаток профессиональных специалистов, которые способны эффективно решать информационные задачи за пределами России. И, наконец, еще одной составляющей указанного комплекса проблем является слабая теоретическая разработка основ современной российской политики в указанной сфере, о чем, к примеру, свидетельствует незначительное количество публикаций по избранной теме.

2. Доктрина информационной безопасности Российской Федерации, принятая в сентябре 2000 г., стала системно-правовой основой для реализации тех целей и задач внешней политики России, которые связаны с защитой внутреннего информационного пространства этого государства и распространением позитивной информации о нем за рубежом. Одобренный президентом России документ не является, безусловно, всеобъемлющим, но, вместе с тем, позволяет сформулировать конкретные направления деятельности как государственных органов власти, так и средств массовой и сетевой информации.

Указанная доктрина может быть использована также в качестве модели для формирования правовой основы реализации целей и задач информационной безопасности Республики Беларуси, учитывая то немаловажное обстоятельство, что внешнеполитические стратегии обеих стран в значительной степени совпадают.

Помимо этого, риски и угрозы, указанные в тексте российской доктрины, могут быть оценены как потенциальная опасность для информационной безопасности нашей страны. Это обусловлено, в первую очередь, тем, что Россия и Беларусь являются стратегическими союзниками, которые должны учитывать взаимные интересы в военно-политической, экономической и иных сферах, включая гуманитарную и культурную.

3. Необходимо также отметить, что в ближайшем будущем кооперация между Республикой Беларусь и Российской Федерацией в области обеспечения информационной безопасности потребует еще более тесного взаимодействия, учитывая стремление третьих стран оказать влияние на информационное пространство Беларуси и России. По этой причине нашей стране понадобится детальное изучение российского опыта в этой сфере, уделяя при этом особое внимание следующим направлениям:

использование структур внешнеполитического аппарата в пропаганде российского образа жизни, традиций, истории и культуры за пределами страны, в том числе и с помощью деятельности международных универсальных и региональных организаций;

координация усилий средств массовой и сетевой информации с целью создания и поддержания позитивного имиджа страны за рубежом;

более эффективное использование новых информационных технологий с целью воздействия на общественное мнение в других государствах, а также для борьбы с проникновением в информационное пространство нашего государства иностранных масс-медиа.

Таким образом, анализ основных принципов и правовой основы осуществления информационной политики Российской Федерации позволяет не только дать объективную оценку степени эффективности обеспечения информационной безопасности России, но и поможет заимствовать отдельные ее элементы для использования в белорусских условиях.

**Список литературы**

Алпатов В.М. 150 языков и политика 1917-2000. Социолингвистические проблемы СССР и постсоветского пространства. М.: «Крафт+», Институт востоковедения РАН, 2000. 224 с.

Артамонов Г.Т., Кристальный Б.В., Курносов И.Н. и др. О концептуальной базе построения в России информационного общества // Информационное общество. 1999. №9. С. 17-19.

Баньков А.С. Информационное обеспечение национальных интересов Беларуси и России // Современные коммуникационные технологии в государственной информационной политике. Доклады и выступления на научно-практической конференции (25 июня 2003 года). С. 10-14.

Вершинин М.С. Политическая коммуникация в информационном обществе. СПб.: Изд-во Михайлова В.А., 2001. 252 c.

Выборы: правовые основы, избирательные технологии. Научн. правовое и практ. пособие / Отв. ред. С.А. Альфер; Науч. ред. М.Ф, Чудаков. Мн.: Тесей, 2000. 304 с.

Грачев Г., Мельник И. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия. М.: Институт философии РАН, 1999.

Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. М.: Институт психологии РАН, 1996.

Емельянов Г. В. Совбез: «правила игры» для всех СМИ должны быть одинаковыми. Интервью для сайта «Страна.Ru» // http://strana.ru/security/state/2001/02/02/981140788. Дата доступа: 12.02.2006.

Гуманитарные исследования в Интернет. Под ред. А. Е. Войскунского. М.: Можайск-Терра, 2001.

Доктрина информационной безопасности Российской Федерации / Чернов А.А. Становление глобального информационного общества: проблемы и перспективы. Приложение 2. М.: «Дашков и К», 2003. С. 158-211.

Концепция формирования информационного общества в России. Одобрена решением Государственной комиссии по информатизации при Государственном комитете Российской Федерации по связи и информатизации от 28 мая 1999 г. // Информационное общество. 1999. №3. С. 3-11.

Крысько В.Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) / Под общ. Ред. А.Е. Тараса. Мн.: Харвест, 1999. 448 с.

Малевич Ю.И. Права человека в мировой политике (вторая половина ХХ века). Мн.: УП «Технопринт», 2001. 256 c.

Окинавская Хартия глобального информационного общества. Принята 22 июля 2000 года лидерами стран «Большой Восьмерки». МОО ВПП ЮНЕСКО «Информация для всех». http://www.ifap.ru/ofdocs/okinhar.htm. 21.03.2006.

Почепцов Г. Г. Информационные войны. М.: Реф-бук, Ваклер, 2000.

Права человека. Учеб. Пособие / Авт.-сост. С.П. Кацубо, И.В. Кучвальская, С.Б. Лугвин. Мн.: Амалфея, 2001. 336 с.

Проблемы информационно-психологической безопасности. Под ред. А. В. Брушлинского, В. Е. Лепского. М.: Институт психологии РАН, 1996.

Расторгуев С. П. Выборы во власть как форма информационной экспансии. М.: Новый век, 1999.

Расторгуев С. П. Программные методы защиты информации в компьютерах и сетях. М.: Яхтсмен, 1993.

Расторгуев С.П. Философия информационной войны. М.: Autopan, 2000.

Трахименок С.А. Безопасность государства. Методолого-правовые аспекты. Мн.: «Хата», 1997. 192 с.

Турарбекова Р.М. Информационное неравенство на Ближнем и Среднем Востоке: мифы и реальность // Белорусский журнал международного права и международных отношений. 2002. № 2. http://beljournal.by.ru/2002/2/index.shtml. 21.04.2006.

Удовик С.Л. Глобализация: семиотические подходы. М.: «Рефл-бук», «Ваклер», 2002. 480 с.

Уткин А.И. Глобализация: процесс осмысления. М.: «Логос», 2001.254 с.

Федотова Л.Н. Паблик Рилейшнз и общественное мнение. СПб: Питер, 2003. 352 с.

Хачатуров К. А. Обеспечение внешнеполитических позиций России в свете Доктрины информационной безопасности Российской Федерации. В сб.: Внешнеполитическая информация и современная дипломатия. Отв. редактор Ю. Б. Кашлев. Редактор Г. Н. Вачнадзе. М.: Дипломатическая академия МИД России, 2001.

Чернов А.А. Становление глобального информационного общества: проблемы и перспективы. М.: «Дашков и К», 2003. 232 c.

Цыгичко В. Н., Смолян Г. Л., Черешкин Д. С. Информационное оружие как геополитический фактор и инструмент силовой политики. М.: ИСА РАН, 1997.

Яковенко А. В. Современная пресс-служба МИД России. В сб.: Внешнеполитическая информация и современная дипломатия. Отв. редактор Ю. Б. Кашлев. Редактор Г. Н. Вачнадзе. М.: Дипломатическая академия МИД России, 2001.

Communications. Russia. CIA. The World Factbook. http://www.cia.gov/cia/publications/factbook/geos/rs.html. Дата доступа: 3.05.2006