**Информационная безопасность России**

Информационная безопасность - важная сфера политики государства. Позиция России по пово­ду ее обеспечения в разных областях (международной и внутренней политике, культуре, идеологи­ческой, духовной, социальной сферах, военном деле, техносфере) отражена в Конституции РФ, Концепциях национальной безопасности РФ и внешней политики РФ, а также в Доктринах инфор­мационной безопасности РФ и Военной, конспективное изложение которых дано в конце статьи. Там же приводится перечень других законодательных и нормативно-правовых документов, регла­ментирующих обеспечение информационной безопасности России.

Из глубины веков дошла до нас притча о встре­че странника с Чумой. Он спросил: «Куда идешь?» «В Багдад. Мне нужно уморить там пять тысяч человек», - был ответ. Через некоторое вре­мя странник, вновь повстречав Чуму, бросил уп­рек: «Ты сказала, что погубишь пять тысяч, а умо­рила пятьдесят». «Нет, - возразила она, - я погу­била только пять тысяч. Остальные умерли от сграха».

С древнейших времен информация играла в жизни людей не только созидательную, но и де­структивную, порой убийственную роль. Сегодня в условиях перехода человечества к новой фазе развития цивилизации - от индустриального к ин­формационному обществу — она превратилась в один из главных факторов прогресса, приобрела ключевое значение для функционирования всех общественных и государственных институтов, адекватного поведения человека. И одновременно стала оружием массового поражения.

**Сфера информации**

Информация — это сведения об окружающем мире и протекающих в нем процессах, восприни­маемые человеком или специальным устройством для его нужд. Она пронизывает все сферы нашей жизни. Без постоянной информационной связи с окружающим миром в принципе невозможна нормальная жизнедеятельность людей и общества.

О влиянии информационных факторов на жиз­недеятельность современного общества говорит тот факт, что созданный человечеством в природ­ной среде «искусственный мир» образуют уже не только техносфера (мир техники, технологий, со­оружений и т.п.), но и информационная сфера, зна­чимость которой непрерывно возрастает для жиз­ни каждого из нас.

Доктрина информационной безопасности РФ определяет **информационную сферу** как совокуп­ность:

♦ информации;

♦ информационной инфраструктуры;

♦ субъектов, осуществляющих сбор, форми­рование, распространение и использование ин­формации;

♦ системы регулирования возникающих при этом общественных отношений.

С нарастанием обмена информацией расширя­ются и возможности для злоупотреблений ею, массовой **дезинформации** - введения в заблужде­ние огромных масс людей ошибочными или пред­намеренно фальсифицированными сведениями. Она широко используется как информационное оружие в политических, экономических и коммер­ческих интересах, во внутриполитической борьбе и на международной арене для ослабления нацио­нально-государственного самосознания граждан, разрушения государств, экспансии и в войнах.

**Противоборство**

Использование информации в конфликтах по­родило **информационное противоборство (ИП)** — взаимное комплексное воздействие сторон друг на друга с целью достижения односторонних преиму­ществ, дезориентации и вынуждения противника к решениям и действиям, ослабляющим и парали­зующим его. Структуру ИП образуют не только радиоэлектронная борьба и компьютерные конф­ликты, но и воздействия на психологическом и мировоззренческом уровнях.

Борьба за достижение целей противоборства реализуется средствами информационной войны. **Информационная война (ИВ)** - это информаци­онное противоборство, в котором для достижения победы над противником в качестве оружия в раз­личных сферах - политической, экономической, социальной, духовной, военной - применяются ин­формация и средства работы с ней.

Это война нового типа, особый вид отношений между государствами и другими противоборству­ющими силами, в которых для разрешения про­тиворечий используются методы и средства си­лового воздействия на информационную сферу. Основной объект ИВ - сознание людей. Она осно­вана на возможности подчинения воли людей, уп­равления и манипулирования общественным сознанием. Информационные войны внутри стра­ны могут происходить при обострении соперни­чества политических противников, особенно -борьбы за власть, в избирательных кампаниях **и** т.п.

Термин ИВ известен давно, но стал широко употребляться американскими военными специ­алистами после войны в Персидском заливе (опе­рация США и их союзников против Ирака «Буря в пустыне» в 1991 г.), в которой информационное оружие показало высокую эффективность. В1992 г. Пентагон издал директиву «Информационная вой­на» (TS 3600.1). В ней намечены основные задачи подготовки к таким войнам.

**Основные цели и задачи информационной войны:**

♦ подавление и уничтожение систем управ­ления противоборствующей стороны;

♦ информационное обеспечение боевых дей­ствий, политики, экономики;

♦ подавление электронных систем против­ника;

♦ психологическое воздействие на личный со­став вооруженных сил и население;

♦ проникновение в информационные силы противника, их ослабление и поражение.

В контексте этих представлений **информаци­онная угроза** — опасность, содержание которой со­ставляет различная информация, пригодная для использования против технических, военных, со­циальных объектов с целью изменения их инте­ресов, потребностей, ориентации в соответствии с целями субъекта воздействия.

Важнейший элемент ИВ - **информационная операция** - наступательная и оборонительная. В них используются такие информационные дей­ствия, как:

♦ стратегическая и оперативная маскировка;

♦ разведка и контрразведка;

♦ дезинформация и контрдезинформация;

♦ блокировка СМИ противника;

♦ контрпропаганда;

♦ психологические операции;

♦ радиоэлектронное противоборство;

♦ защита своей информационной инфра­структуры;

♦ атаки на компьютерные сети противобор­ствующей стороны;

♦ вывод из строя и уничтожение объектов ин­формационной инфраструктуры противника.

Наступательную информационную операцию, преследующую несправедливые и преступные цели, можно определить понятием **информацион­ная агрессия.**

**Информационное оружие (ИО)** — совокупность специально организованной информации, инфор­мационных технологий и средств, применяемых для деструктивных воздействий на сознание и по­ведение населения и военнослужащих, а также информационно-техническую инфраструктуру государства.

**Основные объекты воздействия ИО:**

**♦** отдельные люди, коллективы и социальные системы;

♦ информационно-технические системы и средства работы с информацией.

Воздействующее непосредственно на челове­ка информационное оружие специалисты делят на:

♦ ***информационно-психологическое***- воздей­ствующее на сознание и убеждения человека, его мотивы, потребности, нравственные установки, от­ношение к происходящему (могут использоваться СМИ, Интернет, публичные выступления, беседы, внушение, гипноз и т.п.);

♦ ***энергоииформационное***- влияющее на фи­зиологию и психофизиологию, минуя сознание че­ловека, когда он, не сознавая воздействия, в зави­симости от вида облучения, начинает ощущать по­давленность, тревогу, страх,агрессивность,теряет способность контролировать свои действия.

В качестве средств энергоинформационного воздействия могут применяться радиолокацион­ные системы, космические аппараты, низкочастот­ные и высокочастотные генераторы, биолокаци­онные установки, химические, биологические средства и др.

С помощью энергоинформационного оружия можно изменить поведение людей, в частности — снизить или повысить интенсивность протестных действий (демонстраций, беспорядков) и тем са­мым повлиять на политические и социальные процессы. Ухудшая психофизическое состояние военнослужащих противника, можно снижать их боеспособность и даже побуждать к сдаче в плен. Важнейший результат применения такого ору­жия - необъяснимый, парализующий, «живот­ный» страх.

**Задачи применения ИО:**

**♦** подрыв международного авторитета госу­дарства, его сотрудничества с другими странами;

♦ манипулирование общественным сознани­ем страны-противника, создание атмосферы без­духовности и безнравственности, негативного от­ношения к национальному и культурному насле­дию;

♦ провоцирование политической напряжен­ности и хаоса, инициирование этнических и рели­гиозных столкновений, забастовок, массовых бес­порядков и других акций протеста;

♦ дезинформация населения о работе госу­дарственных органов, подрыв их авторитета, дис­кредитация органов управления;

♦ снижение уровня информационного обеспе­чения органов власти и управления, инспирация ошибочных управленческих решений в системе управления страной, регионом, государственным учреждением, войсками, вооружением и военной техникой, объектами повышенной опасности;

♦ нанесение ущерба жизненно важным инте­ресам государства в политической, экономической, социальной и других сферах.

В арсенале ИО особая роль принадлежит **со­циальной информации** как наиболее массовому средству воздействия, так как ее содержание оп­ределяет помыслы и поступки людей, функцио-

нирование государственных и общественных ин­ститутов, профессиональных, возрастных и этни­ческих групп. Главный ее объект как оружия — сознание индивидуума и различных общностей людей, национальный менталитет, духовно-нрав­ственные и социально-психологические качества личности и общества.

**Сущностные признаки социальной информа­ции:**

**♦** обращенность к личности, социальным группам, классам, социуму в целом как средства воздействия на формирование и развитие чело­веческой психики, индивидуального и массового сознания;

♦ определяющее влияние на социально-эко­номические и политические ориентации людей че­рез воздействие на общественное и индивидуаль­ное сознание;

♦ прямая связь с организацией и эффектив­ностью передачи социального опыта от поколения к поколению с сохранением и упрочением нацио­нальных традиций и обычаев;

♦ конечный результат воздействия на чело­века и общество - поведение людей.

Ресурсы социальной информации могут быть использованы как в прогрессивных, так и деструк­тивных целях. Она может быть исключительно сильным средством деформации индивидуально­го сознания вплоть до изменения психики, доведе­ния ее до болезненного состояния, побудительным мотивом к суицидам, протестным, экстремистским выступлениям, терактам, вооруженным столкно­вениям и т.д.

В общественное с ознание страны -жертвы ин­формационной агрессии целенаправленно внедря­ются ложные представления, которые позволяют агрессору манипулировать ее правительством и народом, захватывать территории и ресурсы, практически не встречая сопротивления, без воо­руженного столкновения обычного типа.

Агрессивное, по целям, использование соци­альной информации может прикрываться лозун­гами о «социально-экономической помощи», «культурном сотрудничестве», «защите демокра­тии» и осуществляться через управляющую эли­ту страны-жертвы, причем не только через ее представителей, ориентированных на агрессора, но и в силу заблуждений политиков, искренне ве­рящих, что действуют во благо своего народа.

**Преимущества информационных средств про­тивоборства** перед обычным оружием:

♦ относительно невысокие затраты;

♦ более широкие возможности скрытого применения;

♦ отсутствие выраженного отличия мероп­риятий информационной войны от других ви­дов информационной деятельности;

♦ меньший риск собственного поражения;

♦ отсутствие экологического ущерба;

♦ сохранение материально-экономической инфраструктуры на территории противника.

Нередко ИО называют «умным», более «гу­манным», но это крайне опасное по своим по­следствиям заблуждение.

Данное оружие страшнее и губительнее для людей, чем любое обычное, «горячее» средство поражения. Оно направлено против самого су­щественного, тонкого и трудно восполнимого в человеке - его психики. И поэтому калечит людей хуже пулевого или осколочного ранения, искажая и опустошая их внутренний мир. Дли­тельное воздействие целенаправленной дезин­формации, хорошо спланированной лжи неиз­бежно подавляет способность к подлинной жизни и порождает наркоманию, психические расстройства, суициды, преступное поведение.

После обычных войн страна и мир способны восстановить общечеловеческий потенциал, пополнить его здоровыми, полноценными деть­ми, а пораженные информационным оружием не способны сформировать следующее поколе­ние психически здоровым. По законам социаль­ной наследственности они могут воспитать только себе подобных. Нервозные, закомплек­сованные, зомбированные люди, как правило, воспитывают таких же невротиков и зомби. Че­ловеческие общности после информационных войн снижают способность восстанавливаться. Тем более эти войны практически не знают окончания. Именно поэтому информационное оружие - это самый страшный и пока еще офи­циально дозволенный вид оружия массового поражения. При нарастающей интенсивности и изощренности его применения у человечества нет будущего. Информационное оружие смер­тоносно и негуманно - оно разрушает душев­ную подлинность человека, лишая его самой ос­новы жизнеспособности.

Защита

Нарастание интенсивности и изощренности применения информационного оружия прида-

ет особое значение способности любого государ­ства защититься от информационной агрессии, обеспечить свою информационную безопас­ность (ИБ). Это понятие сформулировано в Доктрине информационной безопасности РФ: ***«Под информационной безопасностью Россий­ской Федерации*** *понимается состояние защи­щенности ее национальных интересов в ин­формационной сфере, определяющихся сово­купностью сбалансированных интересов личности, общества и государства».*

В литературе встречается более широкое определение: информационная безопасность -такое состояние социума, при котором обеспе­чена надежная и всесторонняя защита личнос­ти, общества и государства от воздействия на них особого вида угроз в форме организован­ных информационных потоков, направленных на деформацию общественного и индивидуаль­ного сознания.

Информационная безопасность тракту­ется:

♦ в широком смысле - как информацион­ная безопасность человека, общества и госу­дарства;

♦ в узком понимании - как защищенность информации и поддерживающей ее инфра­структуры от любых случайных или злонаме­ренных воздействий, а во время войн и воору­женных конфликтов - защита от применения противником информационного оружия.

Мировой опыт требует рассмотрения ново­го аспекта проблемы — информационно-психо­логической безопасности (ИПБ). Ее содержа­ние можно обозначить как защищенность ин­дивидуальной, групповой и общественной психологии и, соответственно, социальных субъектов различных уровней общности, их функциональной организации от разруши­тельного воздействия негативных информаци­онных факторов. Применительно к конкретно­му человеку ИПБ - это защищенность от дест­руктивных информационно-психологических воздействий его внутреннего мира, законных прав, интересов и возможностей адекватного личностного развития в условиях информаци­онного взаимодействия с окружающей средой. Масштабность и мощность воздействия инфор­мационных факторов на психику людей выд­вигают обеспечение ИПБ на уровень общена­циональной проблемы.

Нормативно-правовое обеспечение информационной безопасности

Конституция РФ

(принята всенародным голосованием 12 декабря 1993 г.)

**1. Гарантирует:**

а) *права* каждого гражданина:

♦ свободно искать, получать, передавать, произ­водить и распространять информацию любым закон­ным способом (ст. 29, п. 4);

» на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго име­ни (ст. 23, п. 1), а также предусматривает, что сбор, хранение, использование и распространение инфор­мации о частной жизни лица без его согласия не до­пускаются (ст. 24, п. 1);

♦ на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23, п. 2);

♦ на ознакомление с документами и материала­ми, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом (ст. 24, п. 2);

♦ на достоверную информацию о состоянии ок­ружающей среды и возмещение ущерба, причинен­ного его здоровью или имуществу экологическим пра­вонарушением (ст. 42);

♦ на участие в культурной жизни, пользование учреждениями культуры, доступ к культурным ценно­стям (ст. 44, п. 2);

б) *свободу:*

♦ массовой информации (ст. 29, п. 5);

♦ мысли и слова (ст. 29, п. 1);

*♦* литературного, художественного, научного, тех­нического и других видов творчества, преподавания;

в) *обязанности государства:*

*♦* соблюдать и защищать права и свободы чело­века и гражданина (ст. 2; 6, п. 2 и 3; 15, п. 3 и 4; ст. 17-64; 71, п. в; 72, п. 16; 80, п. 2; 85, п. 2; 114, п. 1е; 125, п. 4), гарантировать равенство граждан (ст. 19, п. 2 и 3);

♦ обеспечивать безопасность страны и граждан (ст. 13, п. 5; 37, п. 3; 71, п. м; 72. п. 16 и 1д; 74, п. 2; 82, п. 1; 83, п. ж; 114, п. 1д);

г) *обязанности органов государственной власти и местного самоуправления, их должностных лиц:*

♦ обеспечить каждому возможность ознакомле­ния с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом (ст. 24, **п.** 2).

**2. Определяет основания для ограничения:** а) *прав и свобод:*

**♦** федеральным законом только в той мере, в какой это необходимо в целях защиты основ кон­ституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспече­ния обороны страны и безопасности государства (ст. 55, п. 3);

♦ в условиях чрезвычайного положения для обес­печения безопасности граждан и защиты конституци­онного строя в соответствии с федеральным конститу­ционным законом с указанием пределов и срока дей­ствия ограничений (ст. 56, п. 1);

б) *права на тайну* переписки, телефонных перего­воров, почтовых, телеграфных и иных сообщений - на основании судебного решения (ст. 23, п. 2);

в) *доступа* к сведениям, составляющим государ­ственную тайну, перечень которых определяется фе­деральным законом (ст. 29, п. **4).**

**3. Запрещает:**

♦ пропаганду или агитацию, возбуждающие соци­альную, расовую, национальную или религиозную не­нависть и вражду (ст. 29, п. 2);

♦ пропаганду социального, расового, националь­ного, религиозного или языкового превосходства (ст. 29, п. 2);

♦ принуждение к выражению своих мнений и убеждений или отказу от них (ст. 29, п. 3);

♦ цензуру (ст. 29, п. 5);

*♦* сокрытие должностными лицами фактов и об­стоятельств, создающих угрозу для жизни и здоровья людей, которое влечет за собой ответственность в со­ответствии с федеральным законом (ст. 41, п. 3).

Концепция национальной безопасности РФ

(утверждена Указом Президента РФ от 17 декабря 1997 г. № 1300 в редакции Указа Президента РФ от 10 января 2000 г. *N°* 24)

Определяет следующие **национальные интересы России в информационной сфере:**

**♦** соблюдение конституционных прав и свобод граждан в области получения и пользования инфор­мацией;

♦ развитие современных телекоммуникацион­ных технологий;

♦ защита государственных информационных ре­сурсов от несанкционированного доступа.

Концепция констатирует: «Усиливаются угрозы национальной безопасности Российской Федерации в информационной сфере». **Серьезную опасность представляют:**

**♦** стремление ряда стран к доминированию в миро­вом информационном пространстве, вытеснению Рос­сии с внешнего и внутреннего информационного рынка;

♦ разработка рядом государств концепции ин­формационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира;

♦ нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, по­лучение несанкционированного доступа к ним.

**В числе задач обеспечения национальной безо­пасности РФ:**

**♦** защита культурного, духовно-нравственного наследия, исторических традиций и норм обществен­ной жизни, сохранение культурного достояния всех народов России;

♦ формирование государственной политики в об­ласти духовного и нравственного воспитания насе­ления;

♦ введение запрета на использование эфирно­го времени в электронных средствах массовой ин­формации для проката программ, пропагандирующих насилие, эксплуатирующих низменные проявления;

♦ противодействие негативному влиянию иност­ранных религиозных организаций и миссионеров.

**Важнейшие задачи обеспечения информацион­ной безопасности РФ:**

**♦** реализация конституционных прав и свобод граждан России в сфере информационной деятель­ности;

ф совершенствование и защита отечественной информационной инфраструктуры, интеграция Рос­сии в мировое информационное пространство;

« противодействие угрозе развязывания проти­воборства в информационной сфере.

Доктрина информационной безопасности РФ

(утверждена Президентом РФ 9 сентября 2000г.,№Пр-1895)

Определяет **виды угроз информационной безо­пасности России:**

а) конституционным правам и свободам чело­века и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

б) информационному обеспечению государствен­ной политики РФ;

в) 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;

г) безопасности информационных и телекоммуни­кационных средств и систем.

**Источники угроз информационной безопаснос­ти РФ:**

а) внешние:

♦ деятельность иностранных политических, эконо­мических, военных, разведывательных и информаци­онных структур, направленная против интересов РФ;

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

♦ обострение международной конкуренции за обладание информационными технологиями и ресур­сами;

♦ деятельность международных террористичес­ких организаций;

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

♦ деятельность космических, воздушных, морс­ких и наземных технических и иных средств (видов) разведки иностранных государств;

♦ разработка рядом государств концепций инфор­мационных войн, предусматривающих создание

средств опасного воздействия на информационные сферы других стран мира, нарушение нормального фун­кционирования информационных и телекоммуникаци­онных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним. б) внутренние:

♦ критическое состояние отечественных отрас­лей промышленности;

♦ неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания госу­дарственных и криминальных структур в информаци­онной сфере, получения криминальными структура­ми доступа к конфиденциальной информации, усиле­ния влияния организованной преступности на жизнь общества, снижения степени защищенности закон­ных интересов граждан, общества и государства в ин­формационной сфере;

♦ недостаточная координация деятельности фе­деральных и региональных органов государственной власти по формированию и реализации единой госу­дарственной политики в области обеспечения инфор­мационной безопасности РФ;

♦ недостаточная разработанность нормативной правовой базы, регулирующей отношения в инфор­мационной сфере, а также недостаточная правопри­менительная практика;

♦ неразвитость институтов гражданского обще­ства и недостаточный государственный контроль над развитием информационного рынка России;

♦ недостаточное финансирование мероприятий по обеспечению информационной безопасности РФ;

♦ недостаточная экономическая мощь государ­ства;

♦ снижение эффективности системы образова­ния и воспитания, недостаточное количество квали­фицированных кадров в области обеспечения инфор­мационной безопасности;

♦ недостаточная активность федеральных орга­нов государственной власти в информировании об­щества о своей деятельности, в разьяснении прини­маемых решений, в формировании открытых государ­ственных ресурсов и развитии системы доступа к ним граждан;

♦ отставание России от ведущих стран мира по уровню информатизации органов государственной вла­сти и местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образо­вания, здравоохранения, сферы услуг и быта граждан.

**Общие методы** обеспечения информационной безопасности РФ:

♦ правовые;

♦ организационно-технические;

♦ экономические.

Так как информационная безопасность РФ - одна из составляющих национальной безопасности, оказывает влияние на защищенность национальных интересов в различных сферах жизнедеятельности общества и госу­дарства, угрозы и методы обеспечения - общие для этих сфер. В то же время в каждой есть свои особенности.

**К числу основных объектов обеспечения инфор­мационной безопасности РФ в сфере духовной жизни относятся:**

**♦** достоинство личности, свобода совести, включая право свободно выбирать, иметь и распространятьрелигиозные и иные убеждения и действовать в соответствии с ними, свобода мысли и слова (за исключением пропаганды или агитации, возбуждаю­щих социальную, расовую, национальную или религи­озную ненависть и вражду), свобода литературного, художественного, научного, технического и других видов творчества, преподавания;

♦ свобода массовой информации;

♦ неприкосновенность частной жизни, личная и семейная тайна;

♦ русский язык как фактор духовного единения народов многонациональной России, язык межгосу­дарственного общения народов СНГ;

. языки, нравственные ценности и культурное наследие народов и народностей РФ;

♦ объекты интеллектуальной собственности.

**Наибольшую опасность в сфере духовной жиз­ни** представляют следующие угрозы информационной безопасности РФ;

♦ деформация системы массового информиро­вания за счет монополизации СМИ и неконтролируе­мого расширения сектора зарубежных СМИ в отече­ственном информационном пространстве;

♦ ухудшение состояния и постепенный упадок объектов российского культурного наследия, включая архивы, музейные фонды, библиотеки, памятники ар­хитектуры, ввиду недостаточного финансирования соответствующих программ и мероприятий;

♦ возможность нарушения общественной ста­бильности, нанесение вреда здоровью и жизни граж­дан вследствие деятельности религиозных объедине­ний, проповедующих религиозный фундаментализм, тоталитарных религиозных сект;

♦ использование СМИ, действующих на террито­рии РФ, зарубежными специальными службами для нанесения ущерба обороноспособности страны и бе­зопасности государства, распространения дезинфор­мации;

♦ неспособность современного гражданского об­щества России обеспечить формирование у подрастаю­щего поколения и поддержание в обществе обществен­но необходимых нравственных ценностей, патриотиз­ма и гражданской ответственности за судьбу страны.

Основные направления обеспечения информаци­онной безопасности РФ в сфере духовной жизни;

♦ развитие в России основ гражданского общества;

♦ создание социально-экономических условий для творческой деятельности и функционирования учреждений культуры;

♦ выработка цивилизованных форм и способов общественного контроля формирования в обществе духовных ценностей, отвечающих национальным ин­тересам страны, воспитанием патриотизма и граж­данской ответственности за ее судьбу;

♦ совершенствование законодательства РФ, ре­гулирующего отношения в области конституционных ограничений прав и свобод человека и гражданина;

» государственная поддержка мероприятий по сохранению и возрождению культурного наследия на­родов и народностей РФ;

» формирование правовых и организационных механизмов обеспечения конституционных прав и свобод граждан, повышения их правовой культуры в интересах противодействия сознательному или не-

преднамеренному нарушению этих конституционных прав и свобод в сфере духовной жизни;

♦ разработка действенных организационно-пра­вовых механизмов доступа СМИ и граждан к откры­той информации о деятельности федеральных орга­нов государственной власти и общественных объеди­нений, обеспечение достоверности сведений о соци­ально значимых событиях общественной жизни, рас­пространяемых через СМИ;

♦ разработка специальных правовых и органи­зационных механизмов недопущения противоправ­ных информационно-психологических воздействий на массовое сознание общества, неконтролируемой коммерциализации культуры и науки, обеспечиваю­щих сохранение культурных и исторических ценнос­тей народов и народностей РФ, рациональное исполь­зование накопленных обществом информационных ресурсов, составляющих национальное достояние;

♦ введение запрета на использование эфирно­го времени электронных СМИ для проката программ, пропагандирующих насилие и жестокость, антиобще­ственное поведение;

♦ противодействие негативному влиянию иност­ранных религиозных организаций и миссионеров.

**Военная доктрина РФ**

(утверждена Указом Президента РФ **от** 21 апреля 2000 г. № 706)

В число мер обеспечения военной безопасности России включает информационные. Среди основных факторов, определяющих военно-политическую об­становку, наряду с распространением ядерного и дру­гих видов оружия массового уничтожения, выделяет информационное противоборство.

Наряду с другими факторами дестабилизирую­щее воздействие на военно-политическую обста­новку оказывает использование субъектами меж­дународных отношений информационных и других (в том числе нетрадиционных) средств и техноло­гий в агрессивных (экспансионистских) целях.

**В числе основных угроз военной безопасности России:**

**♦** внешних - враждебные, наносящие ущерб во­енной безопасности Российской Федерации и ее со­юзников информационные (информационно-техни­ческие, информационно-психологические) действия;

» внутренних - планирование, подготовка и осуще­ствление действий, направленных на дезорганизацию функционирования информационной инфраструктуры.

**К основным задачам Вооруженных сил РФ** и дру­гих войск отнесено обеспечение информационной безопасности.

**В числе основных направлений развития воен­ной организации государства** - совершенствование специального информационного обеспечения Воору­женных сип и других войск, органов управления ими.

При этом указано, что активное информационное противоборство, дезориентация общественного мне­ния в отдельных государствах и мирового сообщества в целом - одна из основных общих черт современной войны.

**Информационная независимость** включена в число основных принципов военно-экономического обеспечения. Концепция внешней политики РФ

(утверждена Президентом РФ 28 июня 2000 г.)

Указывает, что **в отношениях между государства­ми все большую роль наряду с другими играют ин­формационные факторы.** В качестзе **главных со­ставляющих национальной мощи России** на пере­дний план выходят ее интеллектуальные, информаци­онные и коммуникационные возможности, благосос­тояние, образовательный уровень населения и др.

Глобализация мировой экономики наряду с допол­нительными возможностями социально-экономическо­го прогресса порождает и новые опасности, **растет риск зависимости экономической системы и информаци­онного пространства России от воздействия извне.**

Угрозы усугубляются ограниченностью ресурсно­го обеспечения внешней политики РФ, что затрудня­ет успешное отстаивание внешнеэкономических ин­тересов, сужает рамки ее информационного и куль­турного влияния за рубежом.

**Среди приоритетов РФ** в решении глобальных проблем Россия уделяет особое внимание такому ас­пекту укрепления стратегической стабильности, как обеспечение информационной безопасности.

Федеральное законодательство

1. Гражданский кодекс РФ (ч. 1 от 30 ноября 1994 г. № 51-ФЗ с изменениями, ч. 2 от 26 января 1996 г. № 14-ФЗ с изменениями, ч. 3 от 26 ноября 2001 г. № 146-ФЗ с изменениями, ч. 4 от 13 декабря 2006 г. № 230-ФЗ).

2. Уголовный кодекс РФ от 13 июня 1996 г. N9 63-ФЗ (с изменениями).

3. Закон РСФСР «О милиции» от 18 апреля 1991 г. № 1026-1 (с изменениями).

4. Закон РФ «О средствах массовой информации» от 27 декабря 1991 г. № 2124-1 (с изменениями).

5. Закон РФ «О безопасности» от 5 марта 1992 г. № 2446-I (с изменениями).

6. Закон РФ от 23 сентября 1992 г. № 3523-I «О правовой охране программ для электронных вы­числительных машин и баз данных» (с изменениями).

7. Закон РФ «Об авторском праве и смежных пра­вах» от 9 июля 1993 г. № 5351-1 (с изменениями, ут­ратит силу с 1 января 2008 г. в связи с введением в действие ч. 4 Гражданского кодекса).

8. Закон РФ «О государственной тайне» от 21 июля 1993 г. № 5485-I (с изменениями).

9. Федеральный закон «О федеральной фельдъ­егерской связи» от 17 декабря 1994 г. № 67-ФЗ (с изменениями),

10. Федеральный закон «Об органах федеральной службы безопасности в Российской Федерации» от 3 апреля 1995 г. № 40-ФЗ (с изменениями).

11. Федеральный закон «Об оперативно-розыск­ной деятельности» от 12 августа 1995 г. № 144-ФЗ (с изменениями).

12. Федеральный закон «О радиационной безопас­ности населения» от 9 января 1996 г. № 3-ФЗ (с из­менениями).

13. Федеральный закон «О внешней разведке» от 10 января 1996 г. № 5-ФЗ (с изменениями).

14. Федеральный закон «О государственной охра­не» от 27 мая 1996 № 57-ФЗ (с изменениями).

15. Федеральный закон «Об электронной цифро­вой подписи» от 10 января 2002 г. № 1-ФЗ.

16. Федеральный закон «О системе государствен­ной службы Российской Федерации» от 27 мая 2003 г. № 58-ФЗ (с изменениями).

17. Федеральный закон «О связи» от 7 июля 2003 г. № 126-ФЗ (с изменениями).

18. Федеральный закон «О государственной граж­данской службе Российской Федерации» от 27 июля 2004 г. № 79-ФЗ (с изменениями).

19. Федеральный закон «Об архивном деле в Рос­сийской Федерации» от 22 октября 2004 г. № 125-ФЗ.

20. Федеральный закон «Об информации, инфор­мационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.

21. Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.

Концепции, программы, постановления, планы

1. Концепция правовой информатизации России (ут­верждена Указом Президента РФ от 28 июня 1993 г. № 966 с изменениями Указами Президента РФ от 19 ноября 2003 г. № 1365 и от 22 марта 2005 г. № 329).

2. Президентская программа «Правовая инфор­матизация органов государственной власти Россий­ской Федерации» (утверждена Указом Президента РФ от 4 августа 1995 г. № 808).

3. 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.)

4. Федеральная целевая программа «Электронная Россия (2002-2010 годы)» (утверждена постановле­нием Правительства РФ от 28 января 2002 г. № 65 с изменениями распоряжением Правительства РФ от 21 октября 2004 г. № 1355-р; постановлениями Пра­вительства РФ от 26 июля 2004 г. № 380, от 15 августа 2006 г. № 502).

5. Постановление Правительства РФ от 12 февраля 2003 г. № 98 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти»,

6. Концепция использования информационных тех­нологий в деятельности федеральных органов государ­ственной власти до 2010 года (одобрена распоряжени­ем Правительства РФ от 27 сентября 2004 г. № 1244-р).

7. Концепция региональной информатизации до 2010 года (одобрена распоряжением Правительства РФ от 17 июля 2006 г. № 1024-р).

8. Типовая программа развития и использования информационных и телекоммуникационных техноло­гий субъекта РФ (утверждена распоряжением Пра­вительства РФ от 3 июля 2007 г. № 871-р).

9. План подготовки проектов актов, необходимых для реализации Федерального закона «Об информа­ции, информационных технологиях и о защите инфор­мации» (утвержден распоряжением Правительства РФ от 27 июля 2007 г. № 1002-р).

10. План подготовки проектов нормативных актов, необходимых для реализации Федерального закона «О персональных данных» (утвержден распоряжени­ем Правительства РФ от 15 августа 2007 г. № 1055-р).