ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Сибайский институт

**Реферат**

**На тему: Информационная безопасность**.

|  |  |
| --- | --- |
|  | **Выполнил**: студент 1 курса  очно-заочной формы обучения  по направлению «Юриспруденция»  Мажитов Г.А. |

**Содержание**

Введение

1. Понятие и сущность информационной безопасности

2. Национальные интересы в информационной сфере

3. Угрозы нарушения конфиденциальности, целостности, доступности информации

4. Заключение

5. Список использованных источников

**Введение**

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

Информатизация на современном этапе развития человечества является наиболее динамично развивающейся сферой мировой экономики, способной конкурировать по доходности с топливно-энергетическим комплексом, автомобилестроением, производством сельскохозяйственной продукции, и определяет наукоемкость промышленной продукции, ее конкурентоспособность на мировом рынке.

Неправомерное искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляющих системах наносят серьезный материальный и моральный урон многим субъектам (государству, юридическим и физическим лицам), участвующим в процессах автоматизированного информационного взаимодействия, что угрожает экономической безопасности.

Жизненно важные интересы этих субъектов, как правило, заключаются в том, чтобы определенная часть информации, касающаяся их экономических, политических и других сторон деятельности, конфиденциальная коммерческая и персональная информация, была бы постоянно легко доступна и в то же время надежно защищена от неправомерного ее использования: нежелательного разглашения, фальсификации, незаконного тиражирования, блокирования или уничтожения.

Объектом реферата выступила информационная безопасность.

Предметом исследования выступили связи и принципы в сфере обеспечения информационной безопасности как элемента экономической безопасности.

Целью реферата является исследование сущности и содержания информационной безопасности в структуре экономической безопасности.

Для достижения поставленной цели необходимо решить следующие задачи:

Исследовать понятие и сущность информационной безопасности.

Определить национальные интересы в информационной сфере.

Проанализировать угрозы нарушения конфиденциальности, целостности, доступности информации.

**1. Понятие и сущность информационной безопасности**

Информационная безопасность как составляющая часть экономической безопасности требует особого исследования.

Понятие информации первоначально было следующим - это сведения, передаваемые людьми устным, письменным или другим способом (с помощью условных сигналов, технических средств и т.д.) [1]. С середины XX века появляется общенаучное понятие информации, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом; обмен сигналами в животном и растительном мире, передача признаков от клетки к клетке, от организма к организму[2].

Сформулированные к настоящему времени строгие научные определения концентрируют внимание на одном из основных аспектов этого многозначного понятия -- соотношении информации и материи.

Понятие «информационная безопасность» неоднозначно трактуется в современной научной литературе. Можно выделить три принципиально различных подхода к пониманию его содержания. В первом случае информационная безопасность рассматривается как комплекс мероприятий по защите информации и средств ее передачи, хранения, обработки и накопления.

Во втором - как обеспечение защиты от информационных воздействий различного рода или как комплекс мер по противодействию акциям информационной войны.

В третьем случае проблематика информационной безопасности распространяется практически на все сферы жизнедеятельности личности, общества и государства, связанные с производством, преобразованием, потреблением, накоплением и хранением информации независимо от способов и средств осуществления этих процессов (это так называемое расширительное толкование).

Также можно выделить три группы исследователей, которые имеют четко просматриваемые различные тенденции толкования понятия «информационная безопасность». Хотя и внутри этих групп также выделяются несколько иные точки зрения на это понятие.

Ряд исследователей, относимых к первой группе, распространяют понятие информационной безопасности на весь комплекс мероприятий по защите информации[3]. Например, В.И. Ярочкин рассматривает информационную безопасность «как единый целостный механизм, объединяющий все используемые средства, методы и мероприятия, направленные на защиту информации от разглашения, утечки и несанкционированного доступа к ней» [4]. Хотя при этом он отмечает, что появление понятия «информационная безопасность» связано с преодолением обществом отрицательных последствий информатизации. Однако дальнейшего развития в его исследованиях этот тезис не получает.

К первой группе можно также отнести исследователей, которые трактуют информационную безопасность исключительно как безопасность информации, передаваемой (создаваемой, накапливаемой и т.п.) при помощи современных технических средств. И основное внимание при рассмотрении вопросов информационной безопасности уделяют обеспечению безопасности телекоммуникационных и автоматизированных информационных систем, а также информации, хранимой и обрабатываемой на персональных компьютерах[5]. Причем эта тенденция является наиболее распространенной в данной группе. Ее появление вполне закономерно и вызвано рядом обстоятельств, среди которых в первую очередь, по мнению автора, можно отметить следующие:

- основу большей части современных информационных технологий составляют электронные средства обработки, передачи, накопления и хранения информации;

- широкое распространение технических средств, предназначенных для негласного получения информации, которое на начальном этапе не встретило должного противодействия;

- противоречивость и несовершенство правовой базы обеспечения информационной безопасности;

- длительное время подготовка специалистов велась исключительно по техническим вопросам защиты информации;

- незначительное число специалистов гуманитарного профиля (в первую очередь юристов) по данной проблематике;

- недостаточное количество комплексных разработок по проблемам обеспечения информационной безопасности с привлечением специалистов как гуманитарного так и технического профиля.

Интересен подход А.Б. Агапова, который рассматривает информационную безопасность в качестве одного из элементов государственной безопасности, как систему мер по защите «систем и комплексов, аккумулирующих и обрабатывающих спец информацию». Остальные же вопросы он выводит за рамки понятия «информационная безопасность», относя их к «обеспечению национальной безопасности в сфере информатизации и индивидуальных информационных прав» [6].

Основным недостатком всех определений, относимых к данной группе, является то, что авторы не рассматривают информационную безопасность как один из видов безопасности личности, общества и государства, а сводят ее к различным аспектам обеспечения защиты информации.

**2. Национальные интересы в информационной сфере**

Доктрина информационной безопасности РФ дает две классификации национальных интересов в информационной сфере[16]:

По принадлежности.

По важности интересов.

В соответствии с классификацией по принадлежности, национальные интересы - это совокупность интересов личности, интересов общества и интересов государства.

Интересы личности - это реализация конституционных прав на доступ к информации; использование информации в интересах осуществления не запрещенной законом деятельности; физическое, духовное и интеллектуальное развитие; защита информации, обеспечивающей личную безопасность.

Интересы общества - это обеспечение интересов личности в информационной сфере; упрочнение демократии, создание правового, социального государства; достижение и поддержание общественного согласия; духовное обновление России.

Интересы государства - это гармоничное развитие российской информационной инфраструктуры; реализация конституционных прав человека и гражданина в области получения информации и пользования ею; незыблемость конституционного строя, суверенитета и территориальной целостности России; политическая, экономическая и социальная стабильность; безусловное обеспечение законности и поддержание правопорядка; развитие равноправного и взаимовыгодного международного сотрудничества.

В рамках классификации по важности национальных интересов выделяют четыре составляющие национальных интересов РФ в информационной сфере[17].

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. Это предполагает: повышение эффективности использования информационной инфраструктуры в интересах общественного развития, консолидацию российского общества, духовное возрождение многонационального народа РФ; совершенствование системы формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала РФ; обеспечение конституционных прав и свобод человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды; обеспечение конституционных прав и свобод 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; укрепление механизмов правового регулирования отношений в области охраны интеллектуальной собственности, создание условий для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации; обеспечение свободы массовой информации и запрет цензуры; недопущение пропаганды и агитации, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды; запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о государственной политике РФ, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным ресурсам. Это предполагает: укрепление государственных СМИ, расширение их возможности по своевременному доведению достоверной информации до российских и иностранных граждан; ускоренное формирование открытых государственных информационных ресурсов, повышение эффективности их использования.

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. Это предполагает: развитие и совершенствование инфраструктуры единого информационного пространства РФ; развитие отечественной индустрии информационных услуг и повышение эффективности использования государственных информационных ресурсов; развитие производства в РФ конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширение участия России в международной кооперации производителей этих средств и систем; обеспечение государственной поддержки отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

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

Это предполагает: повышение безопасности информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и ИС федеральных органов государственной власти, органов государственной власти субъектов РФ, 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; ускоренное развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью; обеспечение защиты сведений, составляющих государственную тайну; расширение международного сотрудничества РФ в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере. информационный безопасность угроза конфиденциальность

Таким образом, информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности РФ. Национальная безопасность РФ существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

**3. Угрозы нарушения конфиденциальности, целостности, доступности информации**

Существует три разновидности угроз информации:

Угрозы нарушения доступности.

Угрозы нарушения целостности.

Угрозы нарушения конфиденциальности.

Доступность информации - свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

Нарушение доступности представляет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес-целей. Рассмотрим пример: в случае выхода из строя сервера, на котором расположена требуемая для принятия стратегического решения информация, нарушается свойство доступности информации. Аналогичный пример: в случае изоляции по какой-либо причине (выход из строя сервера, отказ каналов связи и т.д.) почтового сервера можно говорить о нарушении доступности услуги «электронная почта». Особо следует отметить тот факт, что причина нарушения доступности информации или информационной услуги не обязательно должна находиться в зоне ответственности владельца услуги или информации. Например, в рассмотренном выше примере с нарушением доступности почтового сервера причина (отказ каналов связи) может лежать вне зоны ответственности администраторов сервера (например, отказ магистральных каналов связи). Также следует отметить, что понятие «доступность» субъективно в каждый момент времени для каждого из субъектов, потребляющих услугу или информацию в данный момент времени. В частности, нарушение доступности почтового сервера для одного сотрудника может означать срыв индивидуальных планов и потерю контракта, а для другого сотрудника той же организации - невозможность получить выпуск свежих новостей.

Целостность информации - существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). Чаще субъектов интересует обеспечение более широкого свойства - достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, т.е. ее неискаженности.

Угрозы нарушения целостности - это угрозы, связанные с вероятностью модификации той или иной информации, хранящейся в информационной системе. Нарушение целостности может быть вызвано различными факторами - от умышленных действий персонала до выхода из строя оборудования.

Причины нарушения целостности информации:

1. Субъективные

1.1. Преднамеренные.

1.1.1. Диверсия (организация пожаров, взрывов, повреждений электропитания и др.).

1.1.2. Непосредственные действия над носителем (хищение, подмена носителей, уничтожение информации).

1.1.3. Информационное воздействие (электромагнитное облучение, ввод в компьютерные системы разрушающих программных средств, воздействие на психику личности и психотропным оружием).

1.2. Непреднамеренные.

1.2.1. Отказы обслуживающего персонала (гибель, длительный выход из строя).

1.2.2. Сбои людей (временный выход из строя).

1.2.3. Ошибки людей.

2. Объективные, непреднамеренные.

2.1. Отказы (полный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения).

2.2. Сбои (кратковременный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения).

2.3. Стихийные бедствия (наводнения, землетрясения, ураганы).

2.4. Несчастные случаи (пожары, взрывы, аварии).

2.5. Электромагнитная несовместимость.

Конфиденциальность - способность системы обеспечивать целостность и сохранность информации ее законных пользователей.

Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда, в связи с угрозой нарушения конфиденциальности, используется термин «утечка». Подобные угрозы могут возникать вследствие «человеческого фактора» (например, случайное делегировании тому или иному пользователю привилегий другого пользователя), сбоев работе программных и аппаратных средств.

Реализация каждой из указанных угроз в отдельности или их совокупности приводит к нарушению информационной безопасности. Можно отметить, что все мероприятия по обеспечению информационной безопасности должны строиться по принципу минимизации указанных угроз.

Также следует отметить, что в современном обществе Интернет предоставляет много возможностей национальным органам и организациям иностранных государств, различным преступным сообществам для осуществления противоправной и иной деятельности, наносящей ущерб Российской Федерации[18]. К их числу можно отнести:

- возможность использования национальными органами и организациями иностранных государств сети для организации нетрадиционных каналов связи;

- использование национальными органами и организациями иностранных государств сети в качестве нового технического канала утечки информации;

- возможность использования среды и технологий Интернет для дезинформирования других государств;

- возможность использования информационных ресурсов Интернет по широкому кругу значимых ситуаций;

- возможность использования информационных ресурсов Интернет в качестве новой и эффективной информационной среды анализа ситуаций со стороны российских правоохранительных органов;

- возможность использования среды Интернет для проведения акций в рамках информационной войны и т.д.

Прежде всего, децентрализованная структура и другие технологические особенности превращают Интернет в принципиально новую среду организации нетрадиционных каналов взаимообмена информацией. Для этих целей могут использоваться следующие режимы обмена (прием-передача) информации в Интернет:

- общение в режиме реального времени на WEB-серверах имеющих «Java-Chat». При выполнении необходимых требований, на компьютер перекачивается специальная Java-программа, осуществляющая кодировку передаваемой информации, а наличие режима «отдельных комнат» исключает возможность контроля переговоров даже со стороны лиц, имеющих аналогичную программу;

- пейджингово - коммутационная программа ICQ. Распространяется свободно, поддержка осуществляется WEB-серверами. Позволяет осуществлять обмен различной информацией (файлы, письма, WWW-адреса, chat) в режиме реального времени, а также off-line переписку через сервера поддержки, при передаче электронной почты не использует почтовый сервер провайдера, уведомляет пользователя о нахождении в настоящий момент в сети Интернет лиц, которых он ранее внес в список контактов;

- установление связи с Web-сервером только по определенному порту, с указанием пароля или полного пути к конкретному документу, выход на сайт только с определенного IP-адреса. Следовательно, информация, размещаемая на данной страничке, будет доступна только для знающих пользователей, и может быть только в определенный отрезок времени;

- удаленные графические интерфейсы (по типу текстовых редакторов), расположенные на специальных сайтах, позволяющие прямо с клавиатуры осуществлять набор различного рода сообщений прямо на удаленном WEB-сервере;

- IP-телефония с использованием свободно распространяемых программ криптозащиты переговоров (IP-phone и др.);

- услуга анонимного доступа в Интернет посредством свободно реализуемых через розничную сеть карточек. Купивший данную карточку из любого места, где есть компьютер, модем и телефон может выйти в ОТКС на время действия карточки, предварительно указав отображенные в ней пароль, логин и необходимые настройки;

- передача пейджинговых сообщений при помощи сети Интернет;

- соединение двух модемов по принципу «точка-точка» с использованием коммутируемых каналов связи, а также аппаратуры уплотнения, позволяющей превращать коммутируемый канал в свободно выделенный, не ущемляя функций первого;

- использование программ криптозащиты передаваемой корреспонденции (PGP и др.), где применены надежные системы шифров;

- использование стеганографии. При помощи данных программ можно шифровать сообщения в картинки различных форматов и в музыкальные файлы. При этом внешне картинки остаются практически неизменными, а музыкальные файлы действующими;

- пересылка сообщений посредством сетей различного уровня (ФИДО и др.);

- «Интернет-кафе», представляющие клиентам возможность разового использования Интернет или электронной почты для получения или отправления единичных сообщений;

- оn-line. Непосредственный прямой доступ к ресурсам серверов сети. Большинство авторов-составителей «страниц» на серверах WWW дают другим пользователям, обратившимся к данной «странице», возможность оставить для них какое-либо сообщение. Это сообщение может быть или коротким, набранным с клавиатуры текстом, или заранее подготовленным файлом;

- chat (в переводе - болтовня). Зная «позывные» - электронный адрес и время работы в сети другого пользователя, можно связаться с ним в это время в режиме chat и вести «диалог» в реальном масштабе времени посредством набора текста на клавиатуре, просматривая на экране дисплея одновременно свои вопросы и получаемые ответы;

- телеконференции. В глобальных сетях существуют целые службы телеконференций всевозможных тематик - «электронные доски объявлений», куда любой пользователь может дать свое объявление и прочитать другие;

- электронная почта, позволяет пользователям обмениваться информацией любого характера, любого объема, путем отправления подготовленных файлов на известный электронный адрес. Существует также система бесплатных электронных почтовых ящиков, услуги которых предлагают множество крупных WEB-серверов. Для получения адреса электронной почты на них достаточно зарегистрироваться на данных серверах под вымышленными установочными данными и в дальнейшем пользоваться им из любой точки доступа (дом, работа, Интернет-кафе и т.д.).

При этом задача организации технического контроля за возможным использованием национальными органами и организациями иностранных государств, различными преступными сообществами перечисленных режимов в отличие от глобальных сетей с централизованной структурой осложняется непостоянством в течение сеанса связи трафика передачи сообщений, что является характерной особенностью децентрализованной структуры Интернет.

Разнообразные способы связи с помощью Интернет позволяют легко устанавливать контакты между людьми независимо от их местонахождения и осуществлять переговоры по любому кругу вопросов. Установление контактов в Интернет может происходить по инициативе как самих национальных органов и организаций иностранных государств, так и другими лицами по их инициативе.

Установление контактов может осуществляться, например, путем рассылки писем-предложений по электронной почте, различного рода анкет, вопросы которых могут так или иначе затрагивать секретные тематики. Прикрытием установления контактов могут быть различные предложения об устройстве на работу, с целью обмена информацией о научных исследованиях и т.д.

Возможно также, что после удаленной атаки через Интернет на компьютер, содержащий сведения конфиденциального характера, пользователю данного компьютера или администратору узла, где был осуществлен взлом, придет сообщение с предложением о противоправной деятельности, а в случае отказа - может быть озвучена угроза сообщения о факте взлома и утечки охраняемой законом информации правоохранительным органам России с соответствующими последствиями.

В этом же плане сеть Интернет предоставляет разнообразные возможности для организации нового нетрадиционного технического канала утечки информации. Ресурсы и технологии Интернет представляют несомненный интерес как новый оперативный источник сведений по широкому кругу оперативно-значимых ситуаций. В начале 90-х годов аналитики национальных органов США обратили внимание на то, что большая часть необходимой информации без особого труда может быть получена через сеть Интернет. Так появилось понятие «компьютерная разведка» и соответственно подразделения, ее осуществляющие.

Сфера их деятельности - так называемая легальная разведка в глобальной сети, организация каналов связи с любым лицом, сбор материалов по оперативно-значимым ситуациям, проведение акций информационной войны, изучение личностных характеристик политиков, ученых, военных, а также важнейших секретоносителей с целью их использования в противоправной деятельности против Российской Федерации.

Таким образом, можно сделать вывод, что существует три разновидности угроз: 1. угрозы нарушения доступности; 2. угрозы нарушения целостности; 3. угрозы нарушения конфиденциальности. Также существует большая угроза информационной безопасности через сеть Интернет.

**4. Заключение**

В ходе исследования было выяснено, что защита информации - есть комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям. А понятие информационной безопасности - это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

Государственная политика обеспечения информационной безопасности РФ основывается на следующих принципах:

Соблюдение Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности РФ.

Открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов РФ и общественных объединений, предусматривающей информирование общества об их деятельности с учетом ограничений, установленных законодательством РФ.

Правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающемся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом.

Приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производстве технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов РФ.

Основными целями обеспечения информационной безопасности Российской Федерации должны быть:

1) выявление на стадии зарождения угроз информационной безопасности Российской Федерации на основных направлениях и линиях деятельности правоохранительных органов, могущих повлечь возникновение кризисных ситуаций и чрезвычайных происшествий, нанесение ущерба жизненно важным интересам Российской Федерации в информационной сфере; прогнозирование угроз информационной безопасности;

2) наиболее полная и своевременная локализация, отражение, нейтрализация и парирование угроз информационной безопасности в интересах:

- обеспечения соблюдения конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечения духовного обновления России, сохранения и укрепления нравственных ценностей общества, традиций патриотизма гуманизма, культурного и научного потенциала страны;

- информационного обеспечения государственной политики Российской Федерации, связанного с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам;

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

- обеспечения защиты информационных ресурсов от несанкционированного доступа, обеспечения безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

**5. Список использованных источников**

1. Конституция РФ (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ) // СЗ РФ. - 2009. - №4. - Ст.445.

2. Уголовный кодекс РФ от 13.06.1996 № 63-ФЗ (с изм. и доп., вступающими в силу с 27.01.2011) // СЗ РФ. - 1996. - № 25. - Ст. 2954.

3. Гражданский кодекс РФ (часть IV) от от 18.12.2006 N 230-ФЗ (ред. от 04.10.2010) // СЗ РФ. - 2006. - № 52 (1 ч.). - Ст. 5496.

4. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (с изм. и доп., вступающими в силу с 27.01.2011) // СЗ РФ. - 2002. - № 1 (ч. 1). - Ст. 1.

5. Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. - 2010. - № 31. - Ст.4193.

6. Доктрина информационной безопасности Российской Федерации (утверждена распоряжением Президента Российской Федерации от 9 сентября 2000 года № Пр-1895) // Российская газета. 28 сентября, 2000.

7. Стратегия национальной безопасности РФ до 2020 г. // Указ Президента РФ от 12.05.2010. № 537.