Содержание:

Введение

Данные считаются итогом отображения и обработки в человеческом сознании многообразия окружающего мира, даёт тебе сведения об окружающих вокруг человека предметах, явлениях природы, деятельности других людей. информационный безопасность угроза

Под охраной данных в данный момент понимается область науки и техники, которая включает совокупность средств, способов и методик человеческой деятельности, нацеленных на обеспечение охраны всех видов информации в предприятиях и организациях различных направлений деятельности и разных форм собственности.

Данные, которые подлежат защите, могут быть представлены на любых носителях, могут храниться, обрабатываться и передаваться различными методами и средствами.

Целями охраны данных являются: возможные предотвращение разглашения, утечки и неправомерного доступа к защищённым сведениям; предупреждение противоправных действий по истреблению, улучшению, изменению, копированию, блокированию данных; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав людей на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранность государственной тайны, конфиденциальности документированной информации в соответствие с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и использовании информационных систем, технологии и средств их снабжения.

Информационная безопасность - это состояние защищенности информационной среды общества, обеспечивающее ее формирование, внедрение и развитие в интересах граждан, организаций, государств.

Угрозы данных выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности.

Цель предоставленной работы состоит в определении видов угроз информационной безопасности и их состава.

1. Понятие и структура угроз защищаемой информации

1.1 Существует три различных подхода в определении угроз, которые включают в себя следующее:

- опасность рассматривается как потенциально существующая ситуация(вероятность, угроза) нарушения сохранности информации, при этом сохранность информации значит, что информация располагается в таком защищённом облике, который способен противостоять хоть каким дестабилизирующим действиям;
- угроза трактуется как явление (событие, случай или возможность их возникновения), следствием которых могут быть нежелательные воздействия на информацию;
- угроза определяется как реальные или потенциально возможные действия, или условия, приводящие к той или другой форме проявления уязвимости информации.

Не важно какая угроза не сводится к чему-то однозначному, она состоит из конкретных взаимосвязанных компонентов, каждый из которых сам по себе не представляет угрозу, но является её частью. Сама опасность возникает лишь при совместном их взаимодействии.

Угрозы защищаемых данных связаны с её уязвимостью, то есть неспособностью информации без помощи других бороться дестабилизирующим действиям, нарушающим её статус. А нарушение статуса защищаемой информации состоит в несоблюдении её физической сохранности, логической структуры и содержания, доступности для юзеров с правами, конфиденциальности (защищённости от сторонних лиц), и выражается по средствам реализации шести форм проявления уязвимости информации.

Прежде всего угроза должна обладать какими-то сущностными проявлениями, а любое проявление принято называть явлением, следственно, одним из показателей и вместе с тем одной из составляющих угроз должно быть явление.

В базе любого явления лежат составляющие причины, которые являются его движущей силой и которые в свою очередность обусловлены определёнными обстоятельствами или предпосылками. Эти предпосылки и обстоятельства относятся к факторам, формирующим вероятность дестабилизирующего воздействия на информацию. Таковым образом, факторы являются одним из её признаком и составляющей угрозы.

Ещё одним определённым показателем угрозы является её направление, то есть итог, к которому может привести дестабилизирующее действие на информацию.

Угроза защищаемой информации – совокупность причин, критерий и условий, формирующих угрозу нарушения статуса информации.

Для раскрытия структуры угроз нужно признаки опасности конкретизировать содержательной долей, которые в свою очередность обязаны открыть характер явлений и факторов, определить их состав и состав критерий.

1.2 К сущностным проявлениям угрозы относятся:

- возникновение дестабилизирующего воздействия на информацию (от кого или чего исходят эти действия);
- виды дестабилизирующего воздействия на данные (каким либо образом);
- методы дестабилизирующего воздействия на данные (какими то приёмами, действиями осуществляются и реализуются виды дестабилизирующего воздействия).

К причинам помимо обстоятельств и событий следует отнести присутствие каналов и способов несанкционированного доступа к конфиденциальной информации для воздействия на информацию со стороны лиц, не имеющих к ней разрешённого доступа.

2. Источники, виды и способы дестабилизирующего воздействия

2.1 К Происхождениям дестабилизирующего воздействия на информацию относятся:

- человечество;
- технические средства показ, хранения, обработки, воспроизведения, передачи информации, средства связи;
- системы обеспечения функционирования технических средств;
- технологические процессы отдельных категорий индустриальных объектов;
- природные явления.

2.2 Самым часто встречаемым, знообразным и рискованным источником дестабилизирующего воздействия на защищаемую информацию являются люди. Это так, потому что воздействие на защищаемую информацию могут оказывать различные категории людей, как работающих, так и неработающих в организации.

К этому источнику относятся:

- сотрудники данной фирмы;
- люди, не работающие в организации, но имеющие доступ к охраняемой информации в силу своей должности;
- лица государственных органов разведки других стран и конкурирующих предприятий;
- сотрудники из криминальных подразделений.

2.3 Технические средства являются вторыми по значимости источником дестабилизирующего воздействия на защищаемую информацию в виду их многообразия.

К этому источнику относятся:

- электронно-вычислительная единица техники;
- электрические и автоматические машинки и копировально-множительная техника;
- средства видео и аудио записывающей и воспроизводящей аппаратуры;
- средства телефонной, телеграфной, факсимильной, громкоговорящей техники;
- устройства радиовещания и телевидения;
- устройства кабельной и радиосвязи.

2.4 Третий источник дестабилизирующего влияния на информацию включает системы.

- Электроснабжения
- Гидронабжения
- Теплоснабжения
- Кондиционирования
- К этому источнику присоединяются вспомогательные электрические и радиоэлектронные системы и средства.

2.5 К четвертому источнику относятся.

- технологические процессы обработки различных объектов ядерной энергетики
- химической промышленности
- радиоэлектроники, а также объекты по изготовлению некоторых видов вооружения и военной техники, которые изменяют естественную структуру окружающей среды.

2.6 Пятый источник – это природные явления, которые включают в себя две составляющие:

- стихийные бедствия;
- атмосферные явления.

Со стороны людей допустимо следующие виды дестабилизирующих воздействий:

- - непосредственное воздействие на носители защищаемой информации;
  - несанкционированное распространение конфиденциальной информации;
  - нарушение режима работы технических устройств отображение хранения, обработки, воспроизведения, передачи данных, устройств связи и технологий обработки информации;
  - вывод из строя технических средств и средств связи;
  - вывод из строя и повреждение режима работы систем обеспечения функционирования названных средств.

2.7 Методы непосредственного действия на носители защищаемой информации могут быть:

- физическое поражение носителя информации;
- создание аварийных ситуации для носителей;
- уничтожение информации с носителей;

- создание искусственных магнитных полей для размагничивания носителей;
- добавление ложной информации.

2.8 Неправомерное распространение закрытой информации может исполняться следующим образом:

- передача информации словами (разбалтывание);
- распространение копий информации;
- демонстрация носителей информации;
- ввод информации в вычислительные сети и системы;
- издание информации в открытой печати;
- использование информации в открытых общественных выступлениях;
- к несанкционированной передаче информации так же относится и утеря носителей информации.

2.9 Видами нарушение работы технических средств и обработки информации могут быть:

- повреждения отдельных частей средств
- нарушение правил использования средств
- внесение изменений в порядок обработки информации
- заражение программ обработки информации вредоносными программами
- показ ошибочных программных команд
- превышение лимитного числа запросов
- создание помех в радио-эфире с помощью дополнительного акустического или шумового фона, изменение (наложение) частот передачи информации
- передача не верных сигналов
- подключение подавляющих фильтров в информационные цепи, цепи питание и заземления
- нарушение режима работы систем обеспечения функционирования средств

2.10 К четвертому виду можно отнести следующие способы:

-
  - неправильный монтаж технических средств;
  - разрушение (поломка) средств, в том числе, повреждения (разрыв) кабельных линий связи;
  - создание аварийных ситуаций для технических средств;
  - отключение средств от сетей питания;
  - вывод из строя или нарушения режима работы систем обеспечения функционирования средств;

- монтирование в электронно-вычислительную технику разрушающих радио и программных закладок.

2.11 Способом вывода из строя и нарушения режима работы систем обеспечения функционирования технических средств можно отнести:

- нарушения правил эксплуатации систем.
- не правильный монтаж систем;
- разрушение или поломка систем или их отдельных элементов;
- создание аварийных ситуаций для систем;
- отключение систем от источников питания;

2.12 К видам дестабилизирующего воздействия второго источника относятся:

- перебои в работе средств;
- создание электромагнитных излучений;
- выход устройств из строя;

2.13 Основными способами дестабилизирующего воздействия второго источника являются:

- технические неисправности и поломки;
- возгорание технических средств;
- выход из строя систем обеспечения функционирования средств;
- воздействия модифицированной структуры находящегося вокруг магнитного поля;
- негативные действия естественных явлений;
- поражение либо деффект носителя данных;
- воздействия вредоных программных продуктов;
- возникновение технических поломок частей средств.

2.14 Видами третьего источника дестабилизирующего воздействия на информацию являются:

- выход систем из строя;
- сбои в работе системы.

2.15 К способам этого вида относятся:

- поломки и аварии;
- возгорания;

- выход из строя источников питания;
- воздействия природных явлений;
- появление технических неисправностей элементов системы;
- изменения естественного радиационного фона окружающей среды (на объектах ядерной энергетики);
- конфигурация химического состава находящейся вокруг окружающей среды (на объектах химической промышленности);
- изменения локальной структуры магнитного поля происходящего вследствие воздействия объектов радиоэлектроники и при изготовлении некоторых видов вооружения и военной технике.

К стихийным(погодным) бедствиям и в тоже время видам воздействия следует отнести землетрясения, наводнения, лавины, ураган (торнадо), оползни, извержения вулканов и прочее.

К атмосферным явлениям (видам воздействия) относятся: гроза, жара, дождь, снег, град, мороз, изменения влажности воздуха и магнитные бури.

3. Виды уязвимости защищаемой информации

3.1 Формы проявления уязвимости защищаемой информации

- кража носителя информации или отображаемой в нём информации (хищение);
- утеря носителя информации ;
- несанкционированное ликвидирование носителя данных или отображённой в нём информации (уничтожение);
- искажение информации (неправомерное изменение, модификация, подделка, фальсификация);
- блокирование информации (временное или постоянное);
- распространение информации (несанкционированное распространение или раскрытие данных).

4. Виды угроз информационной безопасности Российской Федерации

4.1 По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

- угрозы конституционным правам, а так же свободы человека и гражданина в области религиозной жизни и информационной деятельности, каждому, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая промышленность средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка сбыта в ее товаров и выходу этой продукции на вселенский рынок, а также обеспечению накопления, сохранности и эффективного применения Российских информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, а так же создаваемых на территории Российской Федерации.

4.2 Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

- 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;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного

самоуправления, организациями и гражданами требований федерального законодательства, регулирующего дел в информационной сфере;
- неправомерное ограничение доступа людей к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально важной информации;
- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер публичной жизни России от западных информационных структур;
- девальвация духовных ценностей, реклама образцов массовой культуры, основанных на культе насилия (давления), на духовных и нравственных ценностях, противоречащих ценностям, принятым в Российском обществе;
- снижение духовного, нравственного и творческого потенциала народонаселения России, что значительно осложнит подготовку трудовых ресурсов для внедрения и применения новейших технологий, в том числе информационных;
- манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозы безопасности информации

Случайные угрозы

Преднамеренные угрозы

Стихийные бедствия и

аварии

Традиционный шпионаж

и диверсии

Сбои и отказы

технических средств

Несанкционированный

доступ к информации

Ошибки при

разработке

Электромагнитные

излучения и наводки

Алгоритмические

и программные ошибки

Несанкционированная

модификация структур

Ошибки пользователей и обслуживающего персонала

Вредительские

программы

4.3 Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

- монополизация информационного рынка РФ, и его отдельных разделов отечественными и западными информационными структурами;
- запрет деятельности государственных средств широкой информации по информированию отечественной и зарубежной аудитории;
- невысокая эффективность информационного снабжения государственной политики Российской Федерации вследствие недостатка профессионально обученных кадров, неимения системы формирования и осуществления государственной информационной политики.

4.4 Угрозами развитию Российской индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению необходимостью внутреннего рынка в ее продукции и выходу данной продукции на

мировой рынок, а также обеспечению накопления, сохранности и действенного использования российских информационных ресурсов могут являться:

- противодействие доступу России к новым информационным технологиям, взаимовыгодному и равноправному участию наших отечественных производителей в мировом подразделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и взаимосвязи, информационных продуктов, а также создание критерий для усиления технологической зависимости России в области современных информационных технологий;
- закупка органами государственной власти привезенных из других стран средств информатизации, телекоммуникации и взаимосвязи при наличии Российских аналогов, никак не уступающих по своим параметрам зарубежным образцам;
- вытеснение с Российского рынка отечественных производителей средств информатизации, телекоммуникации и связи;
- повышение оттока за рубеж профессионалов и правообладателей интеллектуальной собственности.

4.5 Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

- противоправный сбор и применение информации;
- нарушение технологии переработки информации;
- введение в аппаратные и программные продукты компонентов, реализующих функции, никак не предусмотренные документацией на данные изделия;
- разработка и распространение программных продуктов, нарушающих естественное функционирование информационных и информационно-телекоммуникационных систем, а так же систем защиты информации;
- ликвидирование, повреждение, радио-электронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;

- внедрение электронных приборов для перехвата данных в технические средства обработки, хранения и передачи информации по каналам взаимосвязи, а также в служебные здания органов государственной власти, компаний, учебных учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или кража машинных и других носителей данных;
- перехват информации в сетях передачи информации и на линиях связи, расшифровка данной информации и навязывание ошибочной информации;
- применение Росийских и зарубежных информационных технологий, средств защиты данных, средств информатизации, телекоммуникации и связи при создании и развитии советской информационной инфраструктуры;
- неправомерный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

5. Источники угроз информационной безопасности Российской Федерации

5.1 Источники угроз информационной безопасности Российской Федерации разделяются на внешние и внутренние.

К внешним источникам относятся:

- активность западных политических, экономических, военных, разведывательных и информационных структур, нацеленная против интересов России в сфере информационной деятельности;
- рвение ряда держав к доминированию и ущемлению интересов Российской Федерации в мировом пространстве данных, вытеснению её с внешнего и внутреннего информационных рынков;
- осложнение интернациональной конкурентной борьбе за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- повышение технологического отрыва ведущих государств мира и усиление их способностей по противодействию созданию конкурентоспособных отечественных информационных технологий;

- деятельность космических шатлов, воздушных кораблей, морских и наземных технических и других видов средств разведки зарубежных стран;
- исследование рядом стран концепций информационных войн, непосредственно предусматривающих создание средств опасного воздействия на информационные сферы других держав мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранение информационных ресурсов, получение неправомерного доступа к ним.

5.2 К внутренним источникам относятся:

- неблагоприятная криминогенная обстановка, сопровождаемая тенденциями сращивания муниципальных и криминальных структурах в информационной сфере, получения криминальными структурами доступ к закрытым данным, усиления воздействия организованной преступности на жизнь общества, понижение степени защищенности законных интересов людей, общества и страны в информационной сфере;
- недостающая координация деятельности федеральных органов, органов государственной власти субъектов Российской Федерации по формированию и реализации единообразной государственной политики в сфере обеспечения защиты данных Российской Федерации;
- недостаточная исследованность нормативной законной базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- отсталость ВУЗов гражданского общества и недостающий муниципальный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
- недостаточная финансовая сила страны;
- снижение отдачи системы обучения и воспитания, недастающая численность квалифицированных кадров в области снабжения информационной безопасности;
- недостаточная энергичность федеральных органов государственной власти, субъектов РФ в своевременном информировании общества о своей деятельности, в разъяснении принимаемых решений, в создании открытых государственных ресурсов и развитии системы доступа к ним людей;
- отставание России от крупнейших стран мира по уровню информатизации федеральных органов государственной власти, субъектов Российской

Федерации и органов местного самоуправления, кредитно-экономической сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

6. Угрозы национальной безопасности Российской Федерации

6.1 Общее

Положение отечественной экономики, несовершенство системы организации государственной власти и людского общества, общественно-политическая поляризация русского сообщества и криминализация публичных взаимоотношений, подъем санкционированной преступности и увеличениеповышение масштабов терроризма, осложнение межэтнических и отягощение интернациональных взаимоотношений создают просторный диапозон внутренних и внешних угроз национальной безопасности державы.

В сфере экономики угрозы имеют полный характер и обусловлены до этого только значимым уменьшением внутреннего валового продукта, понижением инвестиционной, инновационной энергичности и научно-технического потенциала, стагнацией аграрного раздела, разбалансированием банковской системы, подъемом наружного и внутреннего муниципального долга, тенденцией к преобладанию в экспортных поставках топливно-сырьевой и энергетической составляющих, а в импортных поставках - продовольствия и вещей употребления, включая вещи первой надобности.

Понижение научно-тех. и технологического потенциала державы, сокращение изучений на стратегически важных направленностях научно-технического становления, вывод из страны профессионалов и интеллектуальной собственности грозят Российской Федерации потерей передовых позиций во всём мире, деградацией наукоемких производств, усилением наружной научно-технической зависимости и подрывом обороноспособности России.

Отрицательные процессы в финансовой экономике лежат в базе сепаратистских устремлений ряда субъектов России. Всё это ведет к ужесточению политической непостоянности, ослаблению одного финансового пространства России и его важных составляющих - производственно-технических и автотранспортных взаимосвязей, финансово-банковской, кредитной и налоговой систем.

Финансовая дезинтеграция, социальная дифференциация сообщества, девальвация духовных ценностей содействует ужесточению напряженности в отношениях ареалов и центра, представляя собой опасность федеративному приспособлению и общественно-финансовому укладу Российской Федерации.

Этноэгоизм, этноцентризм и шовинизм, проявляющиеся в деятельности ряда публичных объединений, а ещё неконтролируемая миграция содействует усилению национализма, политического и религиозного экстремизма, этносепаратизма и творят условия для происхождения инцидентов.

Единое правовое пространство державы размывается вследствие неисполнения принципа приоритета общественных норм Конституции РФ над другими правомерными мерками, федеральных правовых норм над общепризнанными мерками субъектов России, не до конца отлаженности государственного управления на разных уровнях.

Опасность криминализации публичных взаимоотношений, складывающихся в процессе реформирования общественно-политического устройства и финансовой деятельности, приобретает необыкновенную остроту. Нешуточные просчеты, допущенные на исходном шаге проведения реформ в финансовой, военной, правоохранительной и других областях государственной деятельности, понижение системы муниципального регулирования и контроля, несовершенство законной базы и неимение мощной государственной политики в общественной сфере, понижение религиозно-нравственного потенциала общества считаются главными причинами, способствующими подъёму преступности, в особенности ее организованных форм, а также коррупции.

Результаты данных просчетов проявляются в ослаблении правового контролирования из-за обстановки в стране, в сращивании отдельных частей исполнительной и законодательной власти с криминальными структурами, вторжения их в сферу управления банковским делом, огромными производствами, торговыми организациями и товаропроводящими сетями. В связи с этим борьба с санкционированной преступностью и коррупцией имеет не только законный, но и политический нрав.

Масштабы терроризма и спланированной преступности растут вследствие часто сопровождаемого индидентами изменения форм собственности, обострения борьбы из-за власти на базе массовых и этнонационалистических интересов. Неимение действенной системы общественной профилактики правонарушений,

недостаточная правовая и материально-техническая обеспеченность деятельности по предупреждению терроризма и санкционированной преступности, законный скептицизм, вывод из органов снабжения правопорядка обученных сотрудников наращивают степень воздействия данной угрозы на персону, общество и правительство.

Опасность государственной сохранности России в общественной сфере непосредственно создают глубочайшее разделение общества на узкий круг состоятельных и преобладающую массу малоимущих людей, рост удельного веса народа, живущего за чертой бедности, увеличение безработицы.

Угрозой физическому самочувствию цивилизации считаются упадок систем здравоохранения и общественной защиты населения, подъем употребления алкоголя и наркотических средств.

Результатами глубочайшего общественного упадка считаются внезапное сокращение рождаемости и средней длительности жизни в стране, диструкция демографического и общественного состава общества, подрыв трудовых ресурсов как основы развития производства, ослабление базовой ячейки общества - семьи, понижение религиозного, нравственного и творческого потенциала населения.

Углубление кризиса во внутренней политики, социальной и духовной сферах в некоторых случаях может привести к потере демократических покорений.

6.2 Главные опасности в интернациональной сфере обусловлены последующими факторами:

- рвение отдельных стран и межгосударственных объединений, принизить роль существующих механизмов обеспечения международной безопасности, прежде всего ООН и ОБСЕ;
- угроза ослабления политического, финансового и военного влияния России во всём мире;
- улучшение военно-политических блоков и союзов, важнее всего расширение НАТО на восток;
- вероятность возникновения в непосредственной близости от советских границ зарубежных военных баз и объёмных воинских контингентов;
- распределение орудия глобального поражения и средств его доставки;
- понижение интеграционных действий в Содружестве Независимых Государств:

- происхождение и эскалация инцидентов поблизости государственной границы РФ и внешних границ стран - участников Содружества Независимых Государств;
- требования на территорию Российской Федерации.

Угрозы государственной безопасности Российской Федерации в интернациональной сфере появляются в поползновениях остальных стран мешать укреплению России как одного из центров воздействия в многополярном мире, воспрепятствовать реализации государственных интересов и обессилить ее позиции в Европе, на Ближнем Востоке, в Закавказье, Центральной Азии и Азиатско-Тихоокеанском регионе.

Серьезную опасность государственной безопасности России представляет терроризм. Международным терроризмом развязана открытая кампания в целях дестабилизации ситуации в Российской Федерации.

Увеличиваются угрозы национальной безопасности РФ в информационной сфере. Как правило серьезную опасность предполагают собой стремление ряда стран к превосходству в мировом информационном пространстве, вытеснению Российской Федерации с внешнего и внутреннего рынка информации; исследование рядом государств концепции информационных войн, предусматривающей творение средств опасного воздействия на сферы информации других государств мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных данных, получение неправомерного доступа к ним.

Растёт степень и масштабы угроз в военной деятельности.

Взведенный в ранг стратегической доктрины переход НАТО к практике боевых деяний за пределами зоны ответственности блока и в отсутствии запрета Совета Безопасности ООН чреват угрозой дестабилизации всей стратегической обстановки в мире.

Растущий научно-технический отрыв ряда основных держав и усиления их способностей по созданию вооружений и армейской техники нового поколения творят предпосылки качественно нового шага гонки вооружений, коренного изменения форм и способов ведения боевых действий.

Активируется деятельность на местности России зарубежных специальных служб и применяемых ими организаций.

Ужесточению отрицательных тенденций в армейской деятельности содействуют затянувшийся процесс реформирования военной организации и оборонного промышленного комплекса Российской Федерации, нехватка финансирование государственной защиты и несовершенство нормативной законной базы. На современном шаге это имеет место быть в критически невысоком уровне своевременной и военной подготовки Вооруженных Сил России. Остальных войск, воинских формирований и органов, в недопустимом снижении укомплектованности войск современной поставкой вооружения, военной и специальной техникой, в крайней остроте социальных проблем и приводит к ослаблению военной безопасности Российской Федерации целиком.

6.3 Угрозы национальной безопасности и интересам Российской Федерации в пограничной сфере обусловлены:

- финансовой, демографической и цивилизованно-религиозной экспансией сопредельных государств на отечественную местность;
- активизацией деятельности трансграничной разрешённой преступности, а также западных террористических организаций.

Опасность ухудшения экологической ситуации в государстве и истощения ее естественных ресурсов располагается в непосредственной зависимости от состояния экономики и готовности общества понять масштабность и важность этих проблем. Для страны эта опасность особенно велика непосредственно вследствие предпочтительного развития топливно-энергетических разделов финансовой индустрии, неразвитости законодательной базы природоохранной деятельности, неимение либо урезанного применения природосберегающих технологий, низкой экологической культуры. Имеет место быть тенденция к использованию местности РФ в качестве места так сказать переработки и захоронения опасных для окружающей среды материалов и веществ.

В данных обстоятельствах понижение муниципального надзора, недостаточная отдача правовых и финансовых устройств, предостережение и предотвращение экстренных ситуаций повышают риск катастроф техногенного характера во всех отраслях хозяйственной деятельности.

Заключение

Угроза защищаемой информации – совокупность явлений, причин и условий, создающих угрозу нарушения статуса данных.

Наиболее опасным источником дестабилизирующего воздействия на информацию как оказалось является человек, потому как на защищаемую информацию могут воздействовать различные группы людей.

Разнообразие видов и способов дестабилизирующего воздействия на защищаемую информацию говорит о необходимости комплексной системы защиты информации.

Современная Доктрина информационной безопасности Российской Федерации наиболее полно раскрывает виды и источники угроз информационной безопасности, а также методы обеспечения информационной безопасности.

Список использованной литературы

1. Доктрина информационной безопасности Российской Федерации от 5 сентября 2001 г. № Пр-1892.
2. Концепция национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 13 декабря 1993 г. № 1300 (с изменениями и дополнениями от 14 января 2001 г. № 24).
3. Алексинцев А.И. «Безопасность информационных технологий» - 2003г.
4. Живерский А.А. «Защита информации. Проблемы теории и практики» - М.: 1998г.
5. Федеральный Закон РФ N 85-ФЗ. Принят Государственной Думой 03 июля 1992г. "Об участии в международном информационном обмене".