Содержание:

Введение

Под защитой информации понимается сфера науки и техники, включающая совокупность средств, а так же методов человеческой деятельности, которые направлены на обеспечение защиты всех видов информации в организациях и предприятиях работающих в различных сферах деятельности и различных форм собственности.

Информация, которая подлежит защите, может быть представлена на любых носителях, может храниться, обрабатываться и передаваться различными способами и средствами.

Целью защиты информации являются: предотвращение разглашения информации, защита от несанкционированного доступа к охраняемым сведениям; не допущение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальность документов в соответствие с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

Информационная безопасность - это процесс обеспечения конфиденциальности, целостности и доступности информации.

Угроза информации выражается в нарушении ее полноты, конфиденциальности, целостности и доступности.

Цель этой работы заключается в определении видов угроз информационной безопасности и их состава.

1. Понятие и структура угроз защищаемой информации

Существует 3 подхода по нахождению угрозы, которые включают в себя следующее:

1. угроза рассматривается как существующая ситуация (опасность, возможность) нарушения безопасности информации, при этом безопасность информации означает, информация находится в таком защищаемом виде, который может противостоять любым воздействиям, которые могут дестабилизировать ситуацию;
2. угроза определяется как явление (событие, случай или возможность их возникновения), вследствие которого могут появиться ненужные воздействия влияющую на информацию;
3. угроза трактуется как реальное или потенциальное возможное действия, или условие, которое приводит к той или другой форме проявления уязвимости информации.

Любая угроза не сводится к чему-то однозначному, она состоит из точных взаимосвязанных компонентов, каждый из которых по отдельности не составляет угрозу, но является её частью. Сама угроза может возникать только при совокупном их взаимодействии.

Угроза защищаемой информации связана с уязвимостью, то есть неспособностью информации самой противостоять дестабилизирующему воздействию, нарушающим её статус. Статус защищаемой информации состоит в её физической сохранности, логической структуре и содержании, а еще доступности для пользователей, и выражается по средствам реализации, шести форм проявления уязвимости информации.

Угроза должна иметь какие-то особые проявления. Одним из признаков и вместе с тем одной из составляющих угроз должно быть явление.

В любом явлении содержатся составляющие причины, которые являются его силой и которые обусловлены определённым обстоятельствам или предпосылкой. Эти причины и обстоятельства, скорее всего можно отнести к факторам, которые дают возможность при необходимости для дестабилизации воздействия на информацию. Из этого можно сделать вывод, что и факторы являются ещё одним признаком и

составляющей угрозы.

Ещё одним важным признаком угрозы является её направленность,

то есть результат, при котором могли возникнуть дестабилизирующее действия на данные.

Угроза защищаемой информации – явления, факторы и условия, которые создавшие опасность нарушения статуса информации.

Для того что бы раскрыть структуру угрозы нужно знать признаки угроз, а так же конкретизировать содержание, раскрывающее характер явлений, определить состав условий.

К сущностным проявлениям угрозы можно отнести:

1. источник воздействия на информацию, который может вызвать дестабилизацию (от кого или чего исходят эти воздействия);
2. вид дестабилизирующего воздействия на информацию (каким образом);
3. способ дестабилизирующего воздействия на информацию (каким приёмам, действиям осуществляются и реализуются виды дестабилизирующего воздействия).

К факторам относится помимо причин и обстоятельств - наличие канала и метода несанкционированного доступа к закрытым данным, для воздействия на данные со стороны лиц, которые не имеют к ней доступа.

1.2. Источники, виды и способы дестабилизирующего воздействия

К источнику дестабилизирующего воздействия на информацию относятся:

1. человек;
2. хранение, обработка, воспроизведение, передача информации, средство связи, техническое средство отображения,
3. система по обеспечению функционирования технического средства;
4. технологический процесс отдельно взятого промышленного объекта;
5. природные явления.

Самым обычным и простым, многообразным и опасным из источников дестабилизирующего воздействия на конфиденциальную информацию являются люди. Он таков, потому что воздействие на конфиденциальную информацию оказывают различные категории людей, как работающих, так и неработающих на предприятии.

К этому источнику относятся:

1. работники данного предприятия;
2. лица, которые ранее не работали на предприятии, но имеющие доступ к закрытым данным в соответствии служебным положением;
3. работники государственных органов разведки иных стран и конкурирующих организаций;
4. лица из криминального мира.

Технические же возможности являются вторыми по значению источниками, вызывающими дестабилизацию на конфиденциальную информацию в силу их многообразия.

К этому источнику относятся:

1. вычислительная и электронная техника;
2. электрические и автоматические машинки и копировально-множительное оборудование;
3. звукозаписывающее и воспроизводящее оборудование и средства видеосвязи;
4. телефонные, факсимильные, телеграфные средства;
5. радио и телевидение;
6. средства кабельной передачи информации и радиосвязь.

Третий источник, который может вызвать дестабилизацию на данные, включает системы водоснабжения, теплоснабжения, электричества, кондиционирования. Так же к источнику примыкают другие электрические и радиоэлектронные системы и средства.

К 4 источнику можно отнести технологические процессы обработки различные объекты ядерной энергетики, а так же радиоэлектроники, объекты по изготовлению вооружения и военной техники, промышленности в области химии, изменяющую естественную структуру окружающей среды.

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

1. стихийные бедствия;
2. атмосферные явления.

Со стороны человечества возможны следующие виды дестабилизирующих воздействий:

- 1. непосредственное воздействие на носители конфиденциальной информации;
  2. несанкционированное распространение защищаемой информации;
  3. нарушение в работе технических средств хранения, обработки, воспроизведения, передачи данных, средств связи и технологий обработки данных;
  4. выход из строя технических средств и средств связи;
  5. выход из строя и нарушение режима работы системы, которая обеспечивает функционирование названных средств.

Способами, которые непосредственно воздействуют на носители защищаемых данных, являются:

1. разрушение носителя информации;
2. аварийные ситуации для носителей;
3. удаление данных с носителей;
4. создание магнитных полей для размагничивания носителей;
5. внесение заведомо ложной информации.

Несанкционированное распространение конфиденциальной информации осуществляется следующим образом:

1. словесная передача данных;
2. передача копий носителя данных;
3. показ носителей данных;
4. ввод данных в вычислительные сети и системы;
5. опубликование информации в открытой печати;
6. использование данных в открытых публичных выступлениях;
7. к несанкционированному распространению данных может так же принести и потеря носителей информации.

Существуют и другие способы нарушения работы технических средств и обработки данных:

1. повреждение отдельных элементов средств;
2. нарушение правил эксплуатации средств;
3. внесение изменений в обработку информации;
4. заражение программы по обработки информации вирусными программами;
5. выдача неправильной программной команды;
6. превышение расчетных чисел запросов;
7. создание помех в радио-эфире при помощи дополнительного звукового или шумового фона, изменение (наложение) частот передачи данных;
8. передача заведомо ложных сигналов;
9. подключение подавляющего фильтра в информационную цепь, цепь питания и заземление;
10. нарушение в режиме работы системы обеспечения, функционирования средств;

К четвертому виду относятся следующие способы:

- 1. неверный монтаж технического средства;
  2. разрушение (поломка) средства, а так же повреждения (разрыв) кабельных каналов связи;
  3. создания аварийных ситуаций для технических средств;
  4. отключение средств от сетей электроэнергии;
  5. выход из строя или нарушение режима работы систем, обеспечения функционирования средств;
  6. монтирование в электронную и вычислительную технику специально разрушающих радио и программных закладок.

К способу вывода из строя и нарушения режима работы систем обеспечения, функционирования технических средств относятся:

1. не правильная установка систем;
2. разрушение или поломка системы или их отдельных элементов;
3. создание аварийных ситуаций для системы;
4. отключение систем от источников электроэнергии;
5. нарушения правил эксплуатации систем.

К видам дестабилизирующего воздействия второго источника относятся:

1. выход средств из строя;
2. сбои при работе средств;
3. создание электромагнитных волн;

Основным способом дестабилизирующего воздействия второго источника являются:

1. технические поломки, а так же аварии;
2. возгорание технических средств;
3. выход из строя системы обеспечений функционирования средств;
4. плохие воздействия природных явлений;
5. воздействия измененной структуры окружающего магнитного поля;
6. воздействие вирусных программных продуктов;
7. разрушение или поломка носителя информации;
8. возникновение технических неисправностей частей средств.

Видами третьего источника дестабилизирующего воздействия на данные являются:

1. выход системы из строя;
2. сбои при работе систем.

К способам этого вида относятся:

1. поломки, аварии;
2. возгорание;
3. выход из строя источника питания;
4. воздействия природных явлений;
5. появления технических неисправностей элементов системы;
6. изменение естественного радиационного фона окружающей среды (на объектах ядерной энергетики);

1.3. Формы проявления уязвимости защищаемой информации

1. похищение носителя данных или отображаемой в нём информации (кража);
2. потеря носителей информации (утеря);
3. несанкционированные уничтожения носителя информации или отображённой в нём информации (разрушение);
4. искажения информации (несанкционированное изменение, модификации, подделки, фальсификации и т.д.);
5. блокирование информации (временное или постоянное);

6. разглашения информации (несанкционированное распространение или раскрытие информации).

2. Виды угроз информационной безопасности Российской Федерации

По направленности угрозы информационной безопасности РФ подразделяются на такие виды как:

1. угроза конституционному праву и свободе человека и гражданина в области духовной жизни, а так же его деятельности, индивидуальным, групповым и общественным сознанием, духовному возрождению России;
2. угроза в информационном обеспечении государственной политики Российской Федерации;
3. угрозы, которые мешают развитию отечественной индустрии информации, включая индустрию средств по информатизации, а так же телекоммуникации и связи, обеспечение потребностей по внутреннему рынку в ее продукции и выходу этой продукции на мировые рынки, обеспечение накопления, сохранность и эффективность использования отечественного информационного ресурса;
4. угрозы, отвечающие за безопасность информационных и телекоммуникационных средств и систем, которые уже развернуты, так и создаваемые на территории РФ.

Угрозы конституционному праву и свободу человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

1. 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;
2. создания монополии на формирования, получения и распространения данных в РФ, в том числе при помощи телекоммуникационной системы;
3. противодействие, со стороны криминальных структур, реализация гражданами своих конституционных прав на личные и семейные тайны, тайны переписки, телефонных разговоров и иных сообщений;

4. нерациональное, чрезмерное ограничение к доступу общественно нужной информации;
5. противоправные применения специальных средств воздействия на индивидуальное, групповое и общественное сознание;
6. неисполнение федеральными органами государственной власти, органами государственной власти субъектов РФ, органами местного управления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
7. незаконное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного управления, к открытым архивам, к другой открытой социально значимой информации;
8. дезорганизация, а так же разрушение системы по накоплению и сохранению культурных ценностей, включая архивы;
9. нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
10. изгнание российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
11. девальвация духовных ценностей, пропаганда образов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
12. снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;
13. манипулирования информацией (дезинформация, сокрытие или искажение информации).

Угрозой информационному обеспечению государственной политики Российской Федерации являются:

- 1. монополизация информационного рынка РФ;
  2. блокирование работы государственных средств массовой информации по информированию российских и зарубежных граждан;
  3. очень низкая эффективность информационного обеспечения государственной политики РФ вследствие дефицита квалифицированных

рабочих, отсутствие системы по формированию и реализации государственной информационной политики.

Угроза развития отечественной индустрии информации, включает индустрию средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка в ее продукции и выход этой продукции на мировые рынки, а также обеспечение накоплений. Сохранностью и эффективностью использования отечественных информационных ресурсов являются:

1. противодействие доступу Российской Федерации к новым информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационной услуги, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;
2. закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
3. вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
4. уменьшение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозы безопасности информационных и телекоммуникационных средств и систем, развернутых, а так же создаваемых на территории РФ, являются:

1. противоправный сбор и использование данных;
2. нарушения технологии по обработки данных;
3. внедрение в аппаратные и программные изделия компонента, которые реализуют функции, не предусмотренные документами на эти изделия;
4. разработка и распространения программ, которые нарушают функционирование информационных и информационно-телекоммуникационных систем, в том числе системы защиты информации;
5. уничтожение, поломка, радиоэлектронные подавления или разрушения средств и системы обработки информации, телекоммуникации и связи;
6. воздействия на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
7. компрометация ключей и средств, криптографической защиты данных;

8. распространение данных по техническим каналам;
9. внедрение электронного устройства для захвата данных в техническое средство по обработки, хранению и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, организаций, учреждений и предприятий независимо от формы собственности;
10. уничтожение, поломка, разрушение или хищение машинных и других носителей данных;
11. перехват данных в сетях передачи данных и на линиях связи, дешифрование этих данных и навязывание ложной информации;
12. использование некачественных отечественных и зарубежных информационных технологий, средств защиты данных, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
13. несанкционированный доступ к данным, находящихся в банках и базах данных;
14. нарушение законных ограничений на распространение данных.

2.1. Источники угроз информационной безопасности РФ

Источники угроз информационной безопасности РФ делятся на внешние и внутренние.

К внешним можно отнести:

1. работу иностранной экономической, военной, разведывательной, политической, и информационной структуры, направленной против интересов РФ в информационной сфере;
2. стремление стран к доминированию и ущемлению интересов РФ в мировой информационной сфере, работа по вытеснению ее с внешних и внутренних информационных рынков;
3. усиление международной конкурентной борьбы за обладание информационными технологиями и ресурсами;
4. работа разных террористических организаций;
5. увеличение отрыва в технологиях ведущих держав и накопление их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

6. деятельность воздушных, морских и наземных, космических, технических и других средств (видов) разведки разных государств;
7. разработка другими государствами концепции по ведению информационной войны, которые предусматривают создание средств опасного воздействия на информационные сферы других стран, нарушение обычного функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

состояние отечественных отраслей промышленности;

1. Плохое развитие института гражданского общества и не достаточный государственный контроль за развитием информационного рынка России;
2. плохая криминальная обстановка, которая способствует сращиванию государственной и криминальной структуры в информационной жизни, получения криминальными элементами доступа к конфиденциальным данным, усиление влияния преступниками на общую жизнь людей, снижение степени их защищенности, а так же законных интересов, общества и государства в одной информационной сфере;
3. плохая слаженность действий органов государственной власти , а так же органов государственной власти субъектов РФ по формированию и реализации одной государственной политики, которая обеспечит информационную безопасность Российской Федерации;
4. плохая работа по разработке нормативной и правовой базы, которая призвана регулировать отношения в информационной деятельности, а также недостаточная правоприменительная практика;
5. недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
6. недостаточная экономическая мощность государства;
7. неэффективная система образования и воспитания, малое количество квалифицированных кадров в области обеспечения информационной безопасности;
8. недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

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

2.2 Угрозы национальной безопасности РФ

Состояние экономики в нашей стране несовершенно, как и несовершенна система по организации государственной власти и гражданского общества, социально-политическая поляризация российского общества и криминализация общественных отношений, рост организованной преступности и увеличение масштабов терроризма, обострение межнациональных и международных отношений создают широкий спектр внутренних и внешних угроз национальной безопасности страны.

В сфере экономики угрозы имеют комплексный характер, и характеризуются прежде всего существенным сокращением внутреннего валового продукта, снижением инвестиционной, инновационной активности и научно-технического потенциала, стагнацией аграрного сектора, разбалансированием банковской системы, ростом внешнего и внутреннего государственного долга, тенденцией к преобладанию в экспортных поставках топливно-сырьевой и энергетической составляющих, а в импортных поставках - продовольствия и предметов потребления, включая предметы первой необходимости.

Ослабление научно-технического и технологического потенциала страны, сокращение исследований на стратегически важных направлениях научно-технического развития, отток за рубеж специалистов и интеллектуальной собственности угрожают России утратой передовых позиций в мире, деградацией наукоемких производств, усилением внешней технологической зависимости и подрывом обороноспособности России.

Негативные процессы в экономике лежат в основе сепаратистских устремлений ряда субъектов Российской Федерации. Это ведет к усилению политической нестабильности, ослаблению единого экономического пространства России и его важнейших составляющих - производственно-технологических и транспортных связей, финансово-банковской, кредитной и налоговой систем.

Экономическая дезинтеграция, социальная дифференциация общества, девальвация духовных ценностей способствуют усилению по напряженности во взаимоотношениях регионов и центра, представляя собой угрозу федеративному устройству и социально-экономическому укладу Российской Федерации.

Единое правовое пространство страны размывается, вследствие несоблюдения, принципа приоритета норм Конституции Российской Федерации над иными правовыми нормами, федеральных правовых норм над нормами субъектов Российской Федерации, недостаточной отлаженности государственного управления на различных уровнях.

Угроза криминализации общественных отношений, складывающихся в процессе реформирования социально-политического устройства и экономической деятельности, приобретает особую остроту. Серьезные просчеты, ослабление системы государственного регулирования и контроля, несовершенство правовой базы и отсутствие сильной государственной политики в социальной сфере являются основными факторами, способствующими росту преступности, особенно ее организованных форм, а также коррупции.

Последствия этих просчетов проявляются в ослаблении правового контроля за ситуацией в стране, в сращивании отдельных элементов исполнительной и законодательной власти с криминальными структурами, проникновении их в сферу управления банковским бизнесом, крупными производствами, торговыми организациями и сетями. В связи с этим борьба с организованной преступностью и коррупцией имеет не только правовой, но и политический характер.

Масштабы терроризма и организованной преступности зачастую возрастают вследствие сопровождающегося конфликтами изменения форм собственности, обострения борьбы за власть на основе групповых и националистических интересов. Отсутствие нормальной системы по профилактике социальных правонарушений, а так же плохая правовая и материально-техническая обеспеченность сфер по предупреждению терроризма и организованной преступности повышает степень воздействия этой угрозы на личность, общество и государство.

Угроза национальной безопасности России в социальной сфере делают глубокий разрыв общества на узкий круг богатых и массу малообеспеченных граждан, которая преобладает, а так же увеличение населения которые живут за чертой бедности, нарастающая безработица.

Так же угрозой физическому здоровью нации являются кризис в системе здравоохранения и социальной защиты населения, рост употребления алкоголя и наркотиков.

Последствиями этому глубокому социальному кризису являются сокращение рождаемости и общей продолжительности жизни в стране, деформация демографического и социального состава общества, подрыв трудового ресурса стран, как основы развития производства, ослабление фундаментальной ячейки общества - семьи, понижение духовного, нравственного и творческого потенциала населения.

Углубление кризиса во внутриполитической, социальной и духовной сферах страны помогает привести к утрате демократических завоеваний.

Основные угрозы в международной сфере обозначены следующими факторами:

1. Старание отдельных групп и объединений принизить роль межгосударственных механизмов, которые существуют в стране.
2. Риск ослабления экономического, политического и военного влияния РФ по миру;
3. Укрепление военно-политических блоков и союзов, расширение НАТО на восток к примеру;
4. Непосредственная близость от границ РФ иностранных военных баз и крупных воинских соединений;
5. Продажа оружия массового уничтожения и средств по его доставки;
6. Усиление ослабления интеграционного процесса в странах СНГ:
7. Возникновение и эскалация конфликтов вблизи государственной границы Российской Федерации и внешних границ государств - участников Содружества Независимых Государств;
8. притязания на территорию РФ.

Угрозы национальной безопасности РФ в международной сфере проявляются в попытках других государств - противодействовать укреплению государства, как одного из центров влияния в многополярном мире, помехи в реализации национального интереса и ослаблении ее позиции в Европе, на Ближнем Востоке, в Закавказье, Центральной Азии и Азиатско-Тихоокеанском регионе.

Очень серьезную угрозу национальной безопасности Российской Федерации представляет терроризм. Международным терроризмом открытая кампания в целях дестабилизации ситуации в РФ.

Так же увеличивается угроза по национальной безопасности РФ в информационной деятельности. Серьезная опасность идет от других стран которые хотят доминировать. В мировом информационном пространстве вытесняется Россия, как с внешнего и внутреннего информационного рынка; разработка другими государствами 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.

Возрастают уровень и масштабы угрозы даже в военной сфере.

В рамках стратегической доктрины переход НАТО к практике силовых (военных) действий вне зоны ответственности блока череват угрозой дестабилизации всей стратегической обстановки в мире.

Увеличивающийся технологический отрыв других ведущих держав и наращивание их мощностей по созданию вооружений и военной техники нового поколения, могут создать предпосылки качественно нового этапа для гонки вооружений, коренного изменения формы и способа ведения военных действий.

Активизируется деятельность на территории Российской Федерации иностранных спец. служб и используемых ими организаций.

Усилению плохих тенденций в военной сфере способствует затянувшийся процесс по реформированию военной организации и оборонного промышленного комплекса РФ , малое финансирование по национальной обороны и несовершенная нормативной правовой базы. На современном этапе, это может проявляться на критически низком уровне боевой подготовки Вооруженных Сил Российской Федерации, а так же других войск, воинских формирований, в очевидном снижении комплектности войск (сил) новым и современным вооружением, военной техникой, в крайней остроте социальных проблем это и приводит к ослаблению военной безопасности Российской Федерации.

Угрозам национальной безопасности, а так же интересам РФ в пограничной деятельности обусловлены:

1. культурно-религиозной и демографической, экономической, экспансией сопредельных государств на российскую территорию;

2. активизацией работы в трансграничной организованной преступности, а также международных террористических организаций.

Угроза ухудшения в экологической ситуации страны, а так же откачка ее природных ресурсов находится в зависимости от состояния экономики и готовности общества увидеть глобальность и важность этих проблем. У РФ эта угроза очень велика из-за развития топливных и энергетических отраслей промышленности, недостаточная законодательная основа природоохранной деятельности, низкая культура в плане экологии . Имеет место быть тенденция по использованию территории РФ как место для переработки и уничтожение опасных для окружающей среды материалов и отходов .

В таких условиях ухудшение государственного надзора, а так же не работающая экономическая и правовая практика ликвидации и предупреждения чрезвычайных ситуаций могут увеличивать риск катастроф техногенного характера во всех структурах хозяйственной жизнедеятельности.

Заключение

В этой курсовой работе была рассмотрена тема Виды и состав угрозы информационной безопасности. В ней мы поняли, что угроза защищаемой информации – совокупность многих проявлений, факторов и условий, которые создают опасность нарушения статуса информации.

Самым вредным источником по дестабилизации воздействия на данные, является конечно же, человек, потому как на конфиденциальную информацию могут оказывать воздействие разные категории людей.

Разнообразие вида и способа дестабилизирующего воздействия на конфиденциальную информацию говорит о нужности комплексной системы по защите информации.

Современная Доктрина по безопасности РФ в сфере информации хорошо показывает источники угроз информационной безопасности, а также методы обеспечения информационной безопасности.

Список литературы

1. Доктрина по информационной безопасности РФ от 9 сентября 2000 г. № Пр-1895.
2. Концепции по национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 17 декабря 1997 г. № 1300 (с изменениями и дополнениями от 10 января 2000 г. № 24).
3. Алексинцев А.И. «Безопасность информационных технологий» - 2001г. - №3.
4. Живерский А.А. «Защита информации. Проблемы теории и практики» - М.: 1996г.
5. Федеральный Закон РФ N 85-ФЗ. Принят Гос Думой 04 июля 1996г. "Об участии в международном информационном обмене".