Содержание:

Введение

Информация является результатом отображения и обработки в человеческом сознании многообразия окружающего мира, представляет собой сведения об окружающих человека предметах, явлениях природы, деятельности других людей. информационный безопасность угроза

Под защитой информации в настоящее время понимается область науки и техники, которая включает совокупность средств, методов и способов человеческой деятельности, направленных на обеспечение защиты всех видов информации в организациях и предприятиях различных направлений деятельности и различных форм собственности.

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

Целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение 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; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

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

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

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

1. Основные понятия и структура защищаемой информации

1.1 Понятие и структура угроз защищаемой информации

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

- угроза рассматривается как потенциально существующая ситуация (возможность, опасность) нарушения безопасности информации, при этом безопасность информации означает, что информация находится в таком защищённом виде, который способен противостоять любым дестабилизирующим воздействиям;
- 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.

Любая угроза не сводится к чему-то однозначному, она состоит из определённых взаимосвязанных компонентов, каждый из которых сам по себе не составляет угрозу, но является её частью. Сама угроза возникает лишь при совокупном их взаимодействии.

Угрозы защищаемой информации связаны с её уязвимостью, то есть неспособностью информации самостоятельно противостоять дестабилизирующим воздействиям, нарушающим её статус. А нарушение статуса защищаемой информации состоит в нарушении её физической сохранности, логической структуры и содержания, доступности для правомочных пользователей,

конфиденциальности (закрытости для посторонних лиц), и выражается по средствам реализации шести форм проявления уязвимости информации.

Прежде всего угроза должна иметь какие-то сущностные проявления, а любое проявление принято называть явлением, следовательно, одним из признаков и вместе с тем одной из составляющих угроз должно быть явление.

В основе любого явления лежат составляющие причины, которые являются его движущей силой и которые в свою очередь обусловлены определёнными обстоятельствами или предпосылками. Эти причины и обстоятельства относятся к факторам, создающим возможность дестабилизирующего воздействия на информацию. Таким образом, факторы являются её одним признаком и составляющей угрозы.

Ещё одним определённым признаком угрозы является её направленность, то есть результат, к которому может привести дестабилизирующее воздействие на информацию.

Угроза защищаемой информации – совокупность явлений, факторов и условий, создающих опасность нарушения статуса информации.

Для раскрытия структуры угроз необходимо признаки угроз конкретизировать содержательной частью, которые в свою очередь должны раскрыть характер явлений и факторов, определить из состав и состав условий.

К сущностным проявлениям угрозы относятся:

- источник дестабилизирующего воздействия на информацию (от кого или чего исходят эти воздействия);
- виды дестабилизирующего воздействия на информацию (каким образом);
- способы дестабилизирующего воздействия на информацию (какими приёмами, действиями осуществляются и реализуются виды дестабилизирующего воздействия).

1.2 Источники, виды и способы дестабилизирующего воздействия

К источникам дестабилизирующего воздействия на информацию относятся:

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

Самым распространенным, многообразным и опасным источником дестабилизирующего воздействия на защищаемую информацию являются люди. Он таков, потому что воздействие на защищаемую информацию могут оказывать различные категории людей, как работающих, так и неработающих на предприятии.

К этому источнику относятся:

- сотрудники данного предприятия;
- лица, не работающие на предприятии, но имеющие доступ к защищаемой информации в силу служебного положения;
- сотрудники государственных органов разведки других стран и конкурирующих предприятий;
- лица из криминальных структур.

Технические средства являются вторыми по значению источником дестабилизирующего воздействия на защищаемую информацию в силу их многообразия.

К этому источнику относятся:

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

Третий источник дестабилизирующего воздействия на информацию включает системы электроснабжения, водоснабжения, теплоснабжения, кондиционирования. К этому источнику примыкают вспомогательные электрические и радиоэлектронные системы и средства.

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.

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

- стихийные бедствия;
- атмосферные явления.

Со стороны людей возможно следующие виды дестабилизирующих воздействий:

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

Способами непосредственного воздействия на носители защищаемой информации могут быть:

- физическое разрушение носителя информации;
- создание аварийных ситуации для носителей;
- удаление информации с носителей;
- создание искусственных магнитных полей для размагничивания носителей;
- внесение фальсифицированной информации.

Несанкционированное распространение конфиденциальной информации может осуществляться следующим образом:

- словесная передача информации (разбалтывание);
- передача копий носителя информации;
- показ носителей информации;
- ввод информации в вычислительные сети и системы;
- опубликование информации в открытой печати;

- использование информации в открытых публичных выступлениях;

Способами нарушение работы технических средств и обработки информации могут быть:

- повреждения отдельных элементов средств
- нарушение правил эксплуатации средств
- внесение изменений в порядок обработки информации
- заражение программ обработки информации вредоносными программами
- выдача неправильных программных команд
- превышение расчетного числа запросов
- создание помех в радио-эфире с помощью дополнительного звукового или шумового фона, изменение (наложение) частот передачи информации
- передача ложных сигналов
- подключение подавляющих фильтров в информационные цепи, цепи питание и заземления
- нарушение режима работы систем обеспечения функционирования средств

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.

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

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

К видам дестабилизирующего воздействия второго источника относятся:

- выход средств из строя;
- сбои в работе средств;
- создание электромагнитных излучений;

Основными способами дестабилизирующего воздействия второго источника являются:

- технические поломки и аварии;
- возгорание технических средств;
- выход из строя систем обеспечения функционирования средств;
- негативные воздействия природных явлений;
- воздействия измененной структуры окружающего магнитного поля;
- воздействия вредоносных программных продуктов;
- разрушение или повреждение носителя информации;
- возникновение технических неисправностей элементов средств.

Видами третьего источника дестабилизирующего воздействия на информацию являются:

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

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);
- изменения химического состава окружающей среды (на объектах химической промышленности);
- изменения локальной структуры магнитного поля происходящего вследствие деятельности объектов радиоэлектроники и при изготовлении некоторых видов вооружения и военной технике.

К стихийным бедствиям и одновременно видам воздействия следует отнести землетрясения, наводнения, ураган (смерч), оползни, лавины, извержения вулканов.

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

2. Виды и источники угроз информационной безопасности РФ

2.1 Формы проявления уязвимости защищаемой информации

1. хищение носителя информации или отображаемой в нём информации (кража);
2. потеря носителя информации (утеря);
3. несанкционированное уничтожение носителя информации или отображённой в нём информации (разрушение);
4. искажение информации (несанкционированное изменение, модификация, подделка, фальсификация и т.д.);
5. блокирование информации (временное или постоянное);
6. разглашение информации (несанкционированное распространение или раскрытие информации).

2.2 Виды угроз информационной безопасности Российской Федерации

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

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;

- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

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 отношения в информационной сфере;
- неправомерное ограничение доступа граждан 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 значимой 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 общественной жизни России от зарубежных информационных структур;
- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
- снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;
- манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

- - монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
  - блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;
  - низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

- противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления

технологической зависимости России в области современных информационных технологий;
- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

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

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное 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 устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств

информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

2.3 Источники угроз информационной безопасности Российской Федерации

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

критическое состояние отечественных отраслей промышленности;

- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов государственной власти, 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;
- 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.

2.4 Угрозы национальной безопасности Российской Федерации

Состояние отечественной экономики, несовершенство системы 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 осложнение международных отношений создают широкий спектр внутренних и внешних угроз национальной безопасности страны.

В сфере экономики угрозы имеют комплексный характер и обусловлены 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 напряженности во взаимоотношениях регионов и центра, представляя собой угрозу федеративному устройству и социально-экономическому укладу Российской Федерации.

Этноэгоизм, этноцентризм и шовинизм, проявляющиеся в деятельности ряда общественных объединений, а также неконтролируемая миграция способствуют усилению национализма, политического и религиозного экстремизма, этносепаратизма и создают условия для возникновения конфликтов.

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, допущенные на начальном этапе проведения реформ в экономической, военной, правоохранительной и иных областях государственной деятельности, ослабление системы государственного регулирования и контроля, несовершенство правовой базы и отсутствие сильной государственной политики в социальной сфере, снижение духовно-нравственного потенциала общества 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 товаропроводящими сетями. В связи с этим борьба с организованной преступностью и коррупцией имеет не только правовой, но и политический характер.

Масштабы терроризма и организованной преступности возрастают вследствие зачастую сопровождающегося конфликтами изменения форм собственности, обострения борьбы за власть на основе групповых и этнонационалистических интересов.

Отсутствие эффективной системы социальной профилактики правонарушений, недостаточная правовая и материально-техническая обеспеченность деятельности по предупреждению терроризма и организованной преступности, правовой нигилизм, отток из органов обеспечения правопорядка квалифицированных кадров увеличивают степень воздействия этой угрозы на личность, общество и государство.

Угрозу национальной безопасности России в социальной сфере создают глубокое расслоение общества на узкий круг богатых и преобладающую массу

малообеспеченных граждан, увеличение удельного веса населения, живущего за чертой бедности, рост безработицы.

Угрозой физическому здоровью нации являются кризис систем здравоохранения и социальной защиты населения, рост потребления алкоголя и наркотических веществ.

Последствиями глубокого социального кризиса являются резкое сокращение рождаемости и средней продолжительности жизни в стране, деформация демографического и социального состава общества, подрыв трудовых ресурсов как основы развития производства, ослабление фундаментальной ячейки общества - семьи, снижение духовного, нравственного и творческого потенциала населения.

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

Основные угрозы в международной сфере обусловлены следующими факторами:

- стремление отдельных государств и межгосударственных объединений принизить роль существующих механизмов обеспечения международной безопасности, прежде всего ООН и ОБСЕ;
- опасность ослабления политического, экономического и военного влияния России в мире;
- укрепление военно-политических блоков и союзов, прежде всего расширение НАТО на восток;
- возможность появления в непосредственной близости от российских границ иностранных военных баз и крупных воинских контингентов;
- распространение оружия массового уничтожения и средств его доставки;
- ослабление интеграционных процессов в Содружестве Независимых Государств:
- возникновение и эскалация конфликтов вблизи государственной границы Российской Федерации и внешних границ государств - участников Содружества Независимых Государств;
- притязания на территорию Российской Федерации.

Угрозы национальной безопасности Российской Федерации в международной сфере проявляются в попытках других государств противодействовать укреплению России как одного из центров влияния в многополярном мире, помешать реализации национальных интересов и ослабить ее позиции в Европе, на Ближнем Востоке, в Закавказье, Центральной Азии и Азиатско-Тихоокеанском регионе.

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

Усиливаются угрозы национальной безопасности Российской Федерации в информационной сфере. Серьезную опасность представляют собой стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Возведенный в ранг стратегической доктрины переход НАТО к практике силовых (военных) действий вне зоны ответственности блока и без санкции Совета Безопасности ООН чреват угрозой дестабилизации всей стратегической обстановки в мире.

Увеличивающийся технологический отрыв ряда ведущих держав и наращивание их возможностей по созданию вооружений и военной техники нового поколения создают предпосылки качественно нового этапа гонки вооружений, коренного изменения форм и способов ведения военных действий.

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

Усилению негативных тенденций в военной сфере способствуют затянувшийся процесс реформирования военной организации и оборонного промышленного комплекса Российской Федерации, недостаточное финансирование национальной обороны и несовершенство нормативной правовой базы. На современном этапе это проявляется в критически низком уровне оперативной и боевой подготовки Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, в недопустимом снижении укомплектованности войск (сил) современным вооружением, военной и специальной техникой, в крайней остроте социальных проблем и приводит к ослаблению военной безопасности Российской Федерации в целом.

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

- экономической, демографической и культурно-религиозной экспансией сопредельных государств на российскую территорию;
- активизацией деятельности трансграничной организованной преступности, а также зарубежных террористических организаций.

Угроза ухудшения экологической ситуации в стране и истощения ее природных ресурсов находится в прямой зависимости от состояния экономики и готовности общества осознать глобальность и важность этих проблем. Для России эта угроза особенно велика из-за преимущественного развития топливно-энергетических отраслей промышленности, неразвитости законодательной основы природоохранной деятельности, отсутствия или ограниченного использования природосберегающих технологий, низкой экологической культуры. Имеет место тенденция к использованию территории России в качестве места переработки и захоронения опасных для окружающей среды материалов и веществ.

В этих условиях ослабление государственного надзора, недостаточная эффективность правовых и экономических механизмов предупреждения и ликвидации чрезвычайных ситуаций увеличивают риск катастроф техногенного характера во всех сферах хозяйственной деятельности.

3. Меры противодействия угрозам информационной безопасности

3.1 Основные меры противодействия информационным угрозам

По способам осуществления все меры защиты информации, ее носителей и систем ее обработки подразделяются на:

- правовые (законодательные);
- морально-этические;
- технологические;
- организационные (административные и процедурные);
- физические;

- технические (аппаратурные и программные).
- Правовые (законодательные)

К правовым мерам защиты относятся действующие в стране законы, указы и другие нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее получения, обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

Морально-этические

К морально-этическим мерам защиты относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как требования нормативных актов, однако, их несоблюдение ведет обычно к падению авторитета или престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав, кодекс чести и т.п.) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах пользователей и обслуживающего персонала АС.

Технологические

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные обычно на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализации ответственных операций только при наличии разрешений от нескольких должностных лиц, процедур проверки соответствия реквизитов исходящих и входящих сообщении в системах коммутации сообщений,

периодическое подведение общего баланса всех банковских счетов и т.п.

Организационные

Организационные меры зашиты - это меры административного и процедурного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей и обслуживающего персонала с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Меры физической защиты

Физические меры защиты основаны на применении разного рода механических, электро-или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также средств визуального наблюдения, связи и охранной сигнализации. К данному типу относятся также меры и средства контроля физической целостности компонентов АС (пломбы, наклейки и т.п.).

Технические

Технические меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав АС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты.

3.2 Достоинства и недостатки различных видов мер защиты

Законодательные и морально-этические меры

Эти меры определяют правила обращения с информацией и ответственность субъектов информационных отношений за их соблюдение. Законодательные и морально-этические меры противодействия, являются универсальными в том смысле, что принципиально применимы для всех каналов проникновения и НСД к АС и информации. В некоторых случаях они являются единственно применимыми, как например, при защите открытой информации от незаконного тиражирования или при защите от злоупотреблений служебным положением при работе с информацией.

Организационные меры

Очевидно, что в организационных структурах с низким уровнем правопорядка, дисциплины и этики ставить вопрос о защите информации просто бессмысленно. Прежде всего надо решить правовые и организационные вопросы. Организационные меры играют значительную роль в обеспечении безопасности компьютерных систем. Организационные меры - это единственное, что остается, когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый уровень безопасности. Однако, это вовсе не означает, что систему защиты необходимо строить исключительно на их основе, как это часто пытаются сделать чиновники, далекие от технического прогресса.

Этим мерам присущи серьезные недостатки, такие как:

• низкая надежность без соответствующей поддержки физическими, техническими и программными средствами (люди склонны к нарушению любых установленных дополнительных ограничений и правил, если только их можно нарушить);

• дополнительные неудобства, связанные с большим объемом рутинной и формальной деятельности.

Организационные меры необходимы для обеспечения эффективного применения других мер и средств защиты в части, касающейся регламентации действий людей. В то же время организационные меры необходимо поддерживать более надежными физическими и техническими средствами.

Физические и технические средства защиты

Физические и технические средства защиты призваны устранить недостатки организационных мер, поставить прочные барьеры на пути злоумышленников и в максимальной степени исключить возможность неумышленных (по ошибке или халатности) нарушений регламента со стороны персонала и пользователей системы.
Рассмотрим известное утверждение о том, что создание абсолютной (то есть идеально надежной) системы защиты принципиально невозможно.
Даже при допущении возможности создания абсолютно надежных физических и технических средств защиты, перекрывающих все каналы, которые необходимо перекрыть, всегда остается возможность воздействия на персонал системы, осуществляющий необходимые действия по обеспечению корректного функционирования этих* средств (администратора АС, администратора безопасности и т.п.).

Вместе с самими средствами защиты Эти люди образуют так называемое "ядро безопасности". В этом случае, стойкость системы безопасности будет определяться стойкостью персонала из ядра безопасности системы, и повышать ее можно только за счет организационных (кадровых) мероприятий, законодательных и морально-этических мер.
Но даже имея совершенные законы и проводя оптимальную кадровую полигику, все равно проблему защиты до конца решить не удастся.
Во-первых, потому, что вряд ли удастся найти персонал, в котором можно было быть абсолютно уверенным, и в отношении которого невозможно было бы предпринять действий, вынуждающих его нарушить запреты.
Во-вторых, даже абсолютно надежный человек может допустить случайное, неумышленное нарушение.

Основные принципы построения системы защиты ресурсов АС

Построение системы обеспечения безопасности информации в АС и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность
- системность
- комплексность

• непрерывность

• своевременность

• преемственность и непрерывность совершенствования • разумная достаточность

• персональная ответственность

• разделение функций

• минимизация полномочий

• взаимодействие и сотрудничество

• гибкость системы защиты

• открытость алгоритмов и механизмов защиты

• простота применения средств защиты

• научная обоснованность и техническая реализуемость

• специализация и профессионализм

• взаимодействие и координация

• обязательность контроля

Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности информации в АС в соответствии с действующим законодательством в области информации, информатизации и защиты информации, других нормативных актов по безопасности, утвержденных органами государственной власти в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией.

Системность

Системный подход к защите информации в АС предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов,

условий и факторов, существенно значимых для понимания и решения проблемы обеспечения информационной безопасности в АС.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными, технологическими и правовыми мерами.
Одним из наиболее укрепленных рубежей призваны быть средства защиты, реализованные на уровне операционных систем (ОС) СВТ в силу того, что ОС - это та часть компьютерной системы, которая управляет использованием всех ее ресурсов. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

Непрерывность защиты

Защита информации - не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного

хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите АС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки АС в целом и ее системы защиты информации, в частности.
Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования АС и ее системы защиты с учетом изменений в методах и средствах перехвата информации и воздействия на компоненты АС, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

Разделение функций

Принцип Разделения функций, требует, чтобы ни один сотрудник организации не имел полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Все такие операции должны быть разделены на части, и их выполнение должно быть поручено различным сотрудникам. Кроме того, необходимо предпринимать специальные меры по недопущения сговора и разграничению ответственности между этими сотрудниками.

Разумная достаточность (экономическая целесообразность, сопоставимость возможного ущерба и затрат)

Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы АС, в которой эта информация циркулирует. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.
Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока информация находится в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов компьютерной системы и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, в каком это необходимо сотруднику для выполнения его должностных обязанностей.

Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах подразделении. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений обеспечения безопасности информации.

Гибкость системы защиты

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на уже работающую систему, не нарушая процесса ее нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются.

В таких ситуациях свойство гибкости системы защиты избавляет владельцев АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это однако не означает, что информация о конкретной системе защиты должна быть общедоступна.

Простота применения средств защиты

Механизмы зашиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных

трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации.

Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственные лицензии на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными сотрудниками (специалистами подразделений обеспечения безопасности информации).

Взаимодействие и координация

Предполагают осуществление мер обеспечения безопасности информации на основе взаимодействия всех заинтересованных министерств и ведомств, предприятий и организаций при разработке и функционировании АС и ее системы защиты информации, подразделений и специалистов органов МВД специализированных предприятий и организаций в области защиты информации, привлеченных для разработки системы защиты информации в АС, координации их усилий для достижения поставленных целей Гостехкомиссией России (на этапе разработки и внедрения АС) и подразделениями безопасности органов МВД (на этапе функционирования системы).

Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства зашиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Выводы

В арсенале специалистов по информационной безопасности имеется широкий спектр защитных мер: законодательных, морально-этических, административных (организационных), физических и технических (аппаратурных и программных) средств. Все они обладают своими достоинствами и недостатками, которые необходимо знать и правильно учитывать при создании систем защиты.
Все известные каналы проникновения и утечки информации должны быть перекрыты с учетом анализа риска, вероятностей реализации угроз безопасности в конкретной прикладной системе и обоснованного рационального уровня затрат на защиту.
Наилучшие результаты достигаются при системном подходе к вопросам безопасности компьютерных систем и комплексном использовании определенных совокупностей различных мер защиты на всех этапах жизненного цикла системы, начиная с самых ранних стадий ее проектирования.

Заключение

Угроза защищаемой информации – совокупность явлений, факторов и условий, создающих опасность нарушения статуса информации.

Самым опасным источником дестабилизирующего воздействия на информацию является человек, потому как на защищаемую информацию могут оказывать воздействие различные категории 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. Агальцов В.П., Титов В.М. Информатика для экономистов: Учебник. – М: ИД “ФОРУМ”: ИНФРА-М, 2006. – 448 с.

2. Гаврилов М.В. Информатика и информационные технологии: Учебник. – М: Гардарики, 2006. – 655 с.

3. Домарев В.В. Безопасность информационных технологий. – К: ООО “ТИД “ДС”, 2004. – 992 с.

4. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М: Логос; ПБОЮЛ, 2001. – 264 с.

5. Компьютерные системы и сети: Учебное пособие / Под ред. В.П. Косарева и Л.В. Еремина. – М: Финансы и статистика, 2001. – 464 с.

6. Коуров Л.В. Информационные технологии. – Мн.: Амалфея, 2000. – 192 с.

7. Семененко В.А. Информационная безопасность: Учебное пособие. – М: МГИУ, 2005. – 215 с.

8. Шальгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М: ДМК Пресс, 2008. – 544 с.