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

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; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации 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 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.

Значимость это темы, как для меня, так и для общества является то-то за последние годы, компьютерные технологии тесно вошли в нашу жизнь. С доступностью компьютеров, люди также стали активно пользоваться услугами сети Интернет – электронной почтой, Всемирной паутиной, интернет-банкингом. Но при всех достоинствах сети Интернет, в ней таится и масса опасностей. Прежде всего, это угрозы личной и государственной безопасности. Интернет является свободным пространством, где могут легко украсть личные данные, данные банковских карт, в Сети ведутся информационные войны, порождаются информационные конфликты.

Цель данной работы состоит в определении видов угроз информационной безопасности и их состава. Методах и средствах борьбы с ними, входящих в предметную область изучаемого объекта

Задача данной работы - определить сущность информационной безопасности, охарактеризовать основные виды угроз, рассмотреть существующие методы и средства защиты информации.

1 ПОНЯТИЕ И СТРУКТУРА УГРОЗ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

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

1. 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;

2. угроза трактуется как явление (событие, случай или возможность их возникновения), следствием которых могут быть нежелательные воздействия на информацию;

3. 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:

1. источник дестабилизирующего воздействия на информацию (от кого или чего исходят эти воздействия);

2. виды дестабилизирующего воздействия на информацию (каким образом);

3. способы дестабилизирующего воздействия на информацию (какими приёмами, действиями осуществляются и реализуются виды дестабилизирующего воздействия).

К факторам помимо причин и обстоятельств следует отнести наличие каналов и методов 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

К источникам дестабилизирующего воздействия на информацию относятся:

1. люди;

2. технические средства отображения, хранения, обработки, воспроизведения, передачи информации, средства связи;

3. системы обеспечения функционирования технических средств;

4. технологические процессы отдельных категорий промышленных объектов;

5. 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:

а) сотрудники данного предприятия;

б) лица, не работающие на предприятии, но имеющие доступ к защищаемой информации в силу служебного положения;

в) сотрудники государственных органов разведки других стран и конкурирующих предприятий;

г) лица из криминальных структур.

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

К этому источнику относятся:

а) электронно-вычислительная техника;

б) электрические и автоматические машинки и копировально-множительная техника;

в) средства видео и звукозаписывающей и воспроизводящей техники;

г) средства телефонной, телеграфной, факсимильной, громкоговорящей;

д) средства радиовещания и телевидения;

е) 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:

а) стихийные бедствия;

б) атмосферные явления.

Со стороны людей возможно следующие виды дестабилизирующих воздействий:

1. непосредственное воздействие на носители защищаемой информации;

2. несанкционированное распространение конфиденциальной информации;

3. нарушение режима работы технических средств отображение хранения, обработки, воспроизведения, передачи информации, средств связи и технологий обработки информации;

4. вывод из строя технических средств и средств связи;

5. вывод из строя и нарушение режима работы систем обеспечения функционирования названных средств.

Способами непосредственного воздействия на носители защищаемой информации могут быть:

а) физическое разрушение носителя информации;

б) создание аварийных ситуации для носителей;

в) удаление информации с носителей;

г) создание искусственных магнитных полей для размагничивания носителей;

д) внесение фальсифицированной информации.

Несанкционированное распространение конфиденциальной информации может осуществляться следующим образом:

а) словесная передача информации (разбалтывание);

б) передача копий носителя информации;

в) показ носителей информации;

г) ввод информации в вычислительные сети и системы;

д) опубликование информации в открытой печати;

е) использование информации в открытых публичных выступлениях;

ж) к несанкционированному распространению информации может так же принести и потеря носителей информации.

Способами нарушение работы технических средств и обработки информации могут быть:

а) повреждения отдельных элементов средств

б) нарушение правил эксплуатации средств

в) внесение изменений в порядок обработки информации

г) заражение программ обработки информации вредоносными программами

д) выдача неправильных программных команд

е) превышение расчетного числа запросов

ж) создание помех в радио-эфире с помощью дополнительного звукового или шумового фона, изменение (наложение) частот передачи информации

з) передача ложных сигналов

и) подключение подавляющих фильтров в информационные цепи, цепи питание и заземления

к) нарушение режима работы систем обеспечения функционирования средств

К четвертому виду можно отнести следующие способы:

а) неправильный монтаж технических средств;

б) разрушение (поломка) средств, в том числе, повреждения (разрыв) кабельных линий связи;

в) создание аварийных ситуаций для технических средств;

г) отключение средств от сетей питания;

д) вывод из строя или нарушения режима работы систем обеспечения функционирования средств;

е) 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:

а) не правильный монтаж систем;

б) разрушение или поломка систем или их отдельных элементов;

в) создание аварийных ситуаций для систем;

г) отключение систем от источников питания;

д) нарушения правил эксплуатации систем.

К видам дестабилизирующего воздействия второго источника относятся:

а) выход средств из строя;

б) сбои в работе средств;

в) создание электромагнитных излучений;

Основными способами дестабилизирующего воздействия второго источника являются:

а) технические поломки и аварии;

б) возгорание технических средств;

в) выход из строя систем обеспечения функционирования средств;

г) негативные воздействия природных явлений;

д) воздействия измененной структуры окружающего магнитного поля;

е) воздействия вредоносных программных продуктов;

ж) разрушение или повреждение носителя информации;

з) возникновение технических неисправностей элементов средств.

Видами третьего источника дестабилизирующего воздействия на информацию являются:

а) выход систем из строя;

б) сбои в работе системы.

К способам этого вида относятся:

а) поломки и аварии;

б) возгорания;

в) выход из строя источников питания;

г) воздействия природных явлений;

д) появление технических неисправностей элементов системы;

е) изменения естественного радиационного фона окружающей среды (на объектах ядерной энергетики);

ж) изменения химического состава окружающей среды (на объектах химической промышленности);

з) 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.

3 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).

4 ВИДЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

1. угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
2. угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.
3. 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;
4. угрозы информационному обеспечению государственной политики Российской Федерации;

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:

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. создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;

3. 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;

4. нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;

5. противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;

6. 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;

7. 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;

8. дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;

9. нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

10. 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;

11. девальвация духовных ценностей, пропаганда образцов 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. манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

1. монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;

2. блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;

3. 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:

1. 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;

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. 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:

1. противоправные сбор и использование информации;

2. нарушения технологии обработки информации;

3. внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

4. разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

5. уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

6. воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

7. компрометация ключей и средств криптографической защиты информации;

8. утечка информации по техническим каналам;

9. 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;

10. уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

11. перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

12. использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;

13. несанкционированный доступ к информации, находящейся в банках и базах данных;

14. нарушение законных ограничений на распространение информации.

5 ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

К внешним источникам относятся:

1. деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;

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

3. обострение международной конкуренции за обладание информационными технологиями и ресурсами;

4. деятельность международных террористических организаций;

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

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

7. 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;

1. 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;

2. 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;

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

4. неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

5. недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

6. недостаточная экономическая мощь государства;

7. снижение эффективности системы образования и воспитания, недостаточное 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.

6 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:

1. стремление отдельных государств и межгосударственных объединений принизить роль существующих механизмов обеспечения международной безопасности, прежде всего ООН и ОБСЕ;

2. опасность ослабления политического, экономического и военного влияния России в мире;

3. укрепление военно-политических блоков и союзов, прежде всего расширение НАТО на восток;

4. возможность появления в непосредственной близости от российских границ иностранных военных баз и крупных воинских контингентов;

5. распространение оружия массового уничтожения и средств его доставки;

6. ослабление интеграционных процессов в Содружестве Независимых Государств:

7. возникновение и эскалация конфликтов вблизи государственной границы Российской Федерации и внешних границ государств - участников Содружества Независимых Государств;

8. 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.

Возрастают уровень и масштабы угроз в военной сфере.

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:

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

2. 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.

7 МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Противодействие многочисленным угрозам информационной безопасности предусматривает комплексное использование различных способов и мероприятий организационного, правового, инженерно-технического, программно-аппаратного, криптографического характера и т.п.

Организационные мероприятия по защите включают в себя совокупность действий по подбору и проверке персонала, участвующего в подготовке и

эксплуатации программ и информации, строгое регламентирование процесса разработки и функционирования КС.

К правовым мерам и средствам защиты относятся действующие в стране законы, нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушение.

Инженерно-технические средства защиты достаточно многообразны и включают в себя физико-технические, аппаратные, технологические, программные, криптографические и другие средства. Данные средства обеспечивают следующие рубежи защиты: контролируемая территория, здание, помещение, отдельные устройства вместе с носителями информации.

Программно-аппаратные средства защиты непосредственно применяются в компьютерах и компьютерных сетях, содержат различные встраиваемые в КС электронные, электромеханические устройства. Специальные пакеты программ или отдельные программы реализуют такие функции защиты, как разграничение и контроль доступа к ресурсам, регистрация и анализ протекающих процессов, событий, пользователей, предотвращение возможных разрушительных воздействий на ресурсы и другие.

Суть ***криптографической защиты*** заключается в приведении (преобразовании) информации к неявному виду с помощью специальных алгоритмов либо аппаратных средств и соответствующих кодовых ключей.

Для блокирования (парирования) случайных угроз безопасности в КС должен быть решен комплекс задач показанный на рисунке 1.

Рис.1. Задачи защиты информации в КС от случайных угроз

Дублирование информации является одним из самых эффективных способов обеспечения целостности информации. Оно обеспечивает защиту информации, как от случайных угроз, так и от преднамеренных воздействий. Для дублирования информации могут применяться не только несъемные носители информации или специально разработанные для этого устройства, но и обычные устройства со съемными машинными носителями. Распространенными методами дублирования данных в КС являются использование выделенных областей памяти на рабочем диске и зеркальных дисков (жесткий диск с информацией, идентичной как на рабочем диске).

Под ***надежностью*** понимается свойство системы выполнять возложенные на нее функции в определенных условиях обслуживания и эксплуатации . Надежность КС достигается на этапах разработки, производства, эксплуатации. Важным направлением в обеспечении надежности КС является своевременное обнаружение и локализация возможных неисправностей в работе ее технических средств. Значительно сократить возможности внесения субъективных ошибок разработчиков позволяют современные технологии программирования.

Отказоустойчивость – это свойство КС сохранять работоспособность при отказах отдельных устройств, блоков, схем. Известны три основных подхода к созданию отказоустойчивых систем: простое резервирование (использование устройств, блоков, узлов, схем, только в качестве резервных); помехоустойчивое кодирование информации (рабочая информация дополняется специальной контрольной информацией-кодом, которая позволяет определять ошибки и исправлять их); создание адаптивных систем, предполагающих сохранение работоспособного состояния КС при некотором снижении эффективности функционирования в случаях отказов элементов.

Блокировка ошибочных операций . Ошибочные операции в работе КС могут быть вызваны не только случайными отказами технических и программных средств, но и ошибками пользователей и обслуживающего персонала. Для блокировки ошибочных действий используются технические и аппаратно-программные средства, такие как блокировочные тумблеры, предохранители, средства блокировки записи на магнитные диски и другие.

Оптимизация . Одним из основных направлений защиты информации является сокращение числа ошибок пользователей и персонала, а также минимизация последствий этих ошибок. Для достижения этих целей необходимы: научная организация труда, воспитание и обучение пользователей и персонала, анализ и

совершенствование процессов взаимодействия человека и КС.

Минимизация ущерба . Предотвратить стихийные бедствия человек пока не в силах, но уменьшить последствия таких явлений во многих случаях удается. Минимизация последствий аварий и стихийных бедствий для объектов КС может быть достигнута путем: правильного выбора места расположения объекта (вдали от мест, где возможны стихийные бедствия); учета возможных аварий и стихийных бедствий при разработке и эксплуатации КС; организации своевременного оповещения о возможных авариях; обучение персонала борьбе со стихийными бедствиями и авариями, методам ликвидации их последствий.

Основным способом защиты от злоумышленников считается внедрение так называемых средств ААА, или ЗА (аутентификация, авторизация, администрирование).

Авторизация (санкционирование, разрешение) – процедура, по которой пользователь при входе в систему опознается и получает права доступа, разрешенные системным администратором, к вычислительным ресурсам (компьютерам, дискам, папкам, периферийным устройствам).

Авторизация выполняется программой и включает в себя идентификацию и аутентификацию.

Идентификация – предоставление идентификатора, которым может являться несекретное имя, слово, число, для регистрации пользователя в КС. Субъект указывает имя пользователя, предъявленный идентификатор сравнивается с перечнем идентификаторов. Пользователь, у которого идентификатор зарегистрирован в системе, расценивается как правомочный (легальный). Синонимом идентификатора является логин – набор букв и цифр, уникальный для данной системы.

Аутентификация – проверка подлинности, то есть того, что предъявленный идентификатор действительно принадлежит субъекту доступа. Выполняется на основе сопоставления имени пользователя и пароля. После аутентификации субъекту разрешается доступ к ресурсам системы на основе разрешенных ему полномочий.

Наиболее часто применяемыми методами авторизации являются методы, основанные на использовании паролей (секретных последовательностей символов). Пароль можно установить на запуск программы, отдельные действия на

компьютере или в сети. Кроме паролей для подтверждения подлинности могут использоваться пластиковые карточки и смарт-карты.

Администрирование – это регистрация действий пользователя в сети, включая его попытки доступа к ресурсам. Для своевременного пресечения несанкционированных действий, для контроля за соблюдением установленных правил доступа необходимо обеспечить регулярный сбор, фиксацию и выдачу по запросам сведений о всех обращениях к защищаемым компьютерным ресурсам. Основной формой регистрации является программное ведение специальных регистрационных журналов, представляющих собой файлы на внешних носителях информации.

Чаще всего утечка информации происходит путем несанкционированного копирования информации. Эта угроза блокируется:

- методами, затрудняющими считывание скопированной информации. Основаны на создании в процессе записи информации на соответствующие накопители таких особенностей (нестандартная разметка, форматирование, носителя информации, установка электронного ключа), которые не позволяют считывать полученную копию на других накопителях, не входящих в состав защищаемой КС. Другими словами, эти методы направлены на обеспечение совместимости накопителей только внутри данной КС

- методами, препятствующими использованию информации. Затрудняют использование полученных копированием программ и данных. Наиболее эффективным в этом отношении средством защиты является хранение информации в преобразованном криптографическими методами виде. Другим методом противодействия несанкционированному выполнению скопированных программ является использование блока контроля среды размещения программы. Он создается при инсталляции программы и включает характеристики среды, в которой размещается программа, а также средства сравнения этих характеристик. В качестве характеристик используются характеристики ЭВМ или носителя информации.

Для защиты КС от разнообразных вредительских программ (вирусов) разрабатываются специальные антивирусные средства.

Антивирусная программа – часть программного обеспечения, которая устанавливается на компьютер, чтобы искать на дисках и во входящих файлах компьютерные вирусы и удалять их при обнаружении.

Программа обнаруживает вирусы, предлагая вылечить файлы, а при невозможности удалить. Существует несколько разновидностей антивирусных программ:

- сканеры или программы-фаги – это программы поиска в файлах, памяти, загрузочных секторах дисков сигнатур вирусов (уникального программного кода именно этого вируса), проверяют и лечат файлы;

- мониторы (разновидность сканеров) – проверяют оперативную память при загрузке операционной системы, автоматически проверяют все файлы в момент их открытия и закрытия, чтобы не допустить открытия и запись файла, зараженного вирусом; блокирует вирусы;

- иммунизаторы – предотвращают заражение файлов, обнаруживают подозрительные действия при работе компьютера, характерные для вируса на ранней стадии (до размножения) и посылают пользователю соответствующее сообщение;

- ревизоры – запоминают исходное состояние программ, каталогов до заражения и периодически (или по желанию пользователя) сравнивают текущее состояние с исходным;

- доктора – не только находят зараженные вирусами файлы, ни и “лечат” их, то есть удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние;

- блокировщики – отслеживают события и перехватывают подозрительные действия (производимые вредоносной программой), запрещают действие или запрашивают разрешение пользователя.

Эффективным средством противодействия различным угрозам информационной безопасности является закрытие информации методами криптографического (от греч. Kryptos - тайный) преобразования. В результа-те такого преобразования защищаемая информация становится недоступной для ознакомления и непосредственного использования лицами, не имеющими на это полномочий. По виду воздействия на исходную информацию криптографические методы разделены на следующие виды.

Шифрование – процесс маскирования сообщений или данных с целью скрытия их содержания, ограничения доступа к содержанию других лиц. Заключается в

проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов. Для шифрования используются алгоритм преобразования и ключ.

Стеганография – метод защиты компьютерных данных, передаваемых по каналам телекоммуникаций, путем скрытия сообщения среди открытого текста, изображения или звука в файле-контейнере. Позволяет скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. Скрытый файл может быть зашифрован. Если кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы.

Кодирование – замена смысловых конструкций исходной информации (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр. При кодировании и обратном преобразовании используются специальные таблицы или словари, хранящиеся в секрете. Кодирование широко используется для защиты информации от искажений в каналах связи.

Целью ***сжатия информации*** является сокращение объемов информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Поэтому сжатые файлы подвергаются последующему шифрованию.

Рассечение-разнесение заключается в том, что массив защищаемых данных делится (рассекается) на такие элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации. Выделенные таким образом элементы данных разносятся по разным зонам ЗУ или располагаются на различных носителях.

Электронная цифровая подпись (ЭЦП) представляет собой строку данных, которая зависит от некоторого секретного параметра (ключа), известного только подписывающему лицу, и от содержания подписываемого сообщения, представленного в цифровом виде. Используется для подтверждения целостности и авторства данных, нельзя изменить документ без нарушения целостности подписи.

Для блокирования угроз, исходящих из общедоступной системы, используется специальное программное или аппаратно-программное средство, которое получило название ***межсетевой экран*** (МЭ) или fire wall. МЭ позволяет разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Иногда сетевая защита полностью блокирует трафик снаружи внутрь, но разрешает внутренним пользователям свободно связываться с внешним миром. Обычно МЭ защищают внутреннюю сеть предприятия от вторжений из глобальной сети Интернет. Межсетевой экран выполняет четыре основные функции:

- фильтрация данных на разных уровнях;

- использование экранирующих агентов (proxy-серверы), которые являются программами-посредниками и обеспечивают соединение между субъектом и объектом доступа, а затем пересылают информацию, осуществляя контроль и регистрацию;

- трансляция адресов – предназначена для скрытия от внешних абонентов истинных внутренних адресов;

- регистрация событий в специальных журналах. Анализ записей позволяет зафиксировать попытки нарушения установленных правил обмена информацией в сети и выявить злоумышленника.

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.

В данной работе были рассмотрены основные аспекты предметной области информационной безопасности, в частности, некоторые виды угроз безопасности и наиболее распространенные методы борьбы с ними.

В результате реализации угроз информационной безопасности может быть нанесен серьезный ущерб жизненно важным интересам страны в политической, экономической, оборонной и других сферах деятельности, причинен социально-экономический ущерб обществу и отдельным гражданам. Исходя из этого, можно сделать вывод, что информационная безопасность – это комплекс мер, среди которых нельзя выделить наиболее важные.

Актуальность вопросов защиты информации возрастает с каждым годом. Многие считают, что данную проблему можно решить чисто техническими мерами – установкой межсетевых экранов и антивирусных программ. Но для построения надежной защиты в первую очередь необходима информация о существующих угрозах и методах противодействия им. Известный принцип “предупрежден, значит вооружен” работает и в сфере компьютерной безопасности: вовремя распознав угрозу можно не допустить неприятного развития событий. Поэтому нужно соблюдать меры защиты во всех точках сети, при любой работе любых субъектов с информацией.

Однако следует понимать, что обеспечить стопроцентную защиту невозможно. С появлением новых технологий будут появляться и новые угрозы.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895.

2. Концепция 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 Государственной Думой 04 июля 1996г. "Об участии в международном информационном обмене".