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; 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.

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

1. ВИДЫ И СОСТАВ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 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 их 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.

1.2. 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:

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

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

К этому источнику относятся:

1. электронно-вычислительная техника;
2. электрические и автоматические машинки и копировально-множительная техника;
3. средства видео и звукозаписывающей и воспроизводящей техники;
4. средства телефонной, телеграфной, факсимильной, громкоговорящей;

5. средства радиовещания и телевидения;
6. 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:

1. стихийные бедствия;
2. 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:

1. физическое разрушение носителя информации;
2. создание аварийных ситуации для носителей;
3. удаление информации с носителей;
4. создание искусственных магнитных полей для размагничивания носителей;
5. внесение фальсифицированной информации.

Несанкционированное распространение конфиденциальной информации может осуществляться следующим образом:

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

Способами нарушение работы технических средств и обработки информации могут быть:

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

К четвертому виду можно отнести следующие способы:

- 1. неправильный монтаж технических средств;
  2. разрушение (поломка) средств, в том числе, повреждения (разрыв) кабельных линий связи;
  3. создание аварийных ситуаций для технических средств;
  4. отключение средств от сетей питания;
  5. вывод из строя или нарушения режима работы систем обеспечения функционирования средств;
  6. 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:

1. не правильный монтаж систем;
2. разрушение или поломка систем или их отдельных элементов;
3. создание аварийных ситуаций для систем;
4. отключение систем от источников питания;
5. нарушения правил эксплуатации систем.

К видам дестабилизирующего воздействия второго источника относятся:

1. выход средств из строя;
2. сбои в работе средств;
3. создание электромагнитных излучений;

Основными способами дестабилизирующего воздействия второго источника являются:

1. технические поломки и аварии;
2. возгорание технических средств;
3. выход из строя систем обеспечения функционирования средств;
4. негативные воздействия природных явлений;
5. воздействия измененной структуры окружающего магнитного поля;
6. воздействия вредоносных программных продуктов;
7. разрушение или повреждение носителя информации;
8. возникновение технических неисправностей элементов средств.

Видами третьего источника дестабилизирующего воздействия на информацию являются:

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

К способам этого вида относятся:

1. поломки и аварии;
2. возгорания;
3. выход из строя источников питания;
4. воздействия природных явлений;
5. появление технических неисправностей элементов системы;

6. изменения естественного радиационного фона окружающей среды (на объектах ядерной энергетики);
7. изменения химического состава окружающей среды (на объектах химической промышленности);
8. 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.

1.3. 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).

2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ

2.1. 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 информационному обеспечению государственной политики Российской Федерации;
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 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:

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.

2.2. 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.

2.3. 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.

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.

Парирование угрозам безопасности информации всегда носит недружественный характер по отношению к пользователям и обслуживающему персоналу. Это происходит из-за того, что любая система защиты, по определению, всегда налагает ограничения на работу организационного и технического характера. Поэтому одним из основных принципов создания системы комплексной защиты информации должен стать принцип максимальной дружественности. То есть не надо вводить запреты там, где без них можно обойтись, а если уж и вводить ограничения, то перед этим посмотреть, как это можно сделать с минимальными неудобствами для пользователя. При этом следует учесть не только совместимость создаваемой системы комплексной защиты с используемой операционной и программно-аппаратной структурой корпоративной сети и сложившимися традициями фирмы.

Вплотную к этой проблеме стоит принцип прозрачности. Корпоративной сетью пользуются не только высококлассные программисты. Кроме того, основное назначение корпоративной сети является обеспечение производственных потребностей пользователей, то есть – работа с информацией. Поэтому система защиты информации должна работать в «фоновом» режиме, быть «незаметной» и не мешать пользователям в основной работе, но при этом выполнять все возложенные на нее функции.

Принцип превентивности. Надо всегда помнить, что устранение последствий проявления угроз безопасности информации потребует значительных финансовых, временных и материальных затрат, гораздо больших, чем затраты на создание системы комплексной защиты информации.

Принцип оптимальности. Оптимальный выбор соотношения между различными методами и способами парирования угрозам безопасности информации при принятии решения позволит в значительной степени сократить расходы на создание системы защиты информации.

Принцип адекватности. Принимаемые решения должны быть дифференцированы в зависимости от важности, частоты и вероятности возникновения угроз безопасности информации, степени конфиденциальности самой информации и ее коммерческой стоимости.

Принцип системного подхода к построению системы защиты информации позволяет заложить комплекс мероприятий по парированию угрозам безопасности информации уже на стадии проектирования корпоративной сети, обеспечив оптимальное сочетание организационных и инженерно-технических мер защиты информации. Важность реализации этого принципа основана на том, что оборудование действующей незащищенной корпоративной сети средствами защиты информации сложнее и дороже, чем изначальное проектирование и построение ее в защищенном варианте.

Принцип адаптивности. Система защиты информации должна строиться с учетом возможного изменения конфигурации сети, числа пользователей и степени конфиденциальности и ценности информации. При этом, введение каждого нового элемента сети или изменение действующих условий не должно снижать достигнутый уровень защищенности в целом.

Принцип доказательности. При создании системы защиты информации необходимо соблюдение организационных мер внутри сети, включая привязку логического и физического рабочих мест друг к другу, и применения специальных аппаратно-программных средств идентификации, аутентификации, подтверждения подлинности информации. Реализация данного принципа позволяет сократить расходы на усложнение системы, например, применять цифровую электронную подпись только при работе с удаленными и внешними рабочими местами, и терминалами, связанными с корпоративной сетью по каналам связи.

Эти принципы должны быть положены в основу при выборе направлений обеспечения безопасности корпоративной сети, функций и мер защиты информации.

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".

6. Акулов О.А, Медведев Н.В. Информатика: базовый курс. - М.: Омега - Л, 2005

7. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. - СПб.: Питер, 2006 - 703 с: ил.

7. Информатика в экономике: Учебное пособие/ Под ред. Профессора Б.Е. Одинцова, профессора А.Н Романова. - М.: Вузовский учебник, 2008. - 478 с.

9. Кагаловский М.Р. Энциклопедия технологий баз данных. - М.:Финансы и статистика, 2002. -800 с.

10. Лабораторный практикум для студентов II курса всех специальностей. - М.: Вузовский учебник, 2006. - 94 с.

ПРИЛОЖЕНИЕ

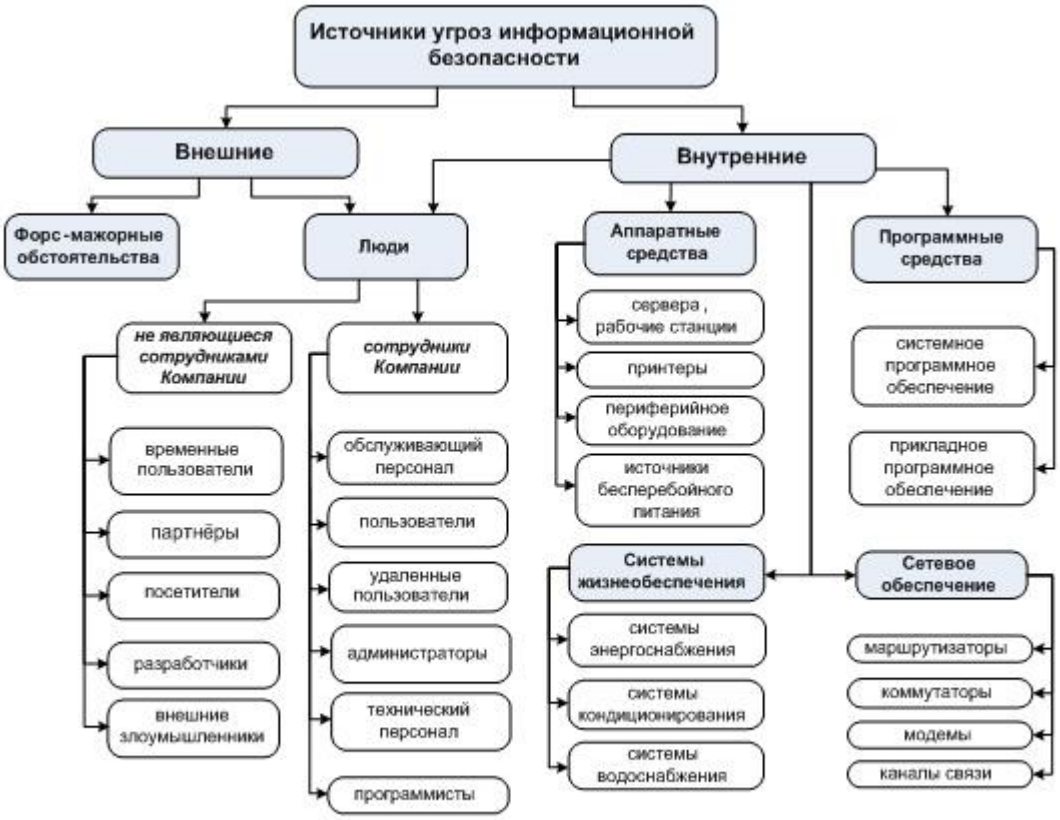
Таблица 1

Источники основных информационных угроз для России

Источник: «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)».

Таблица 2

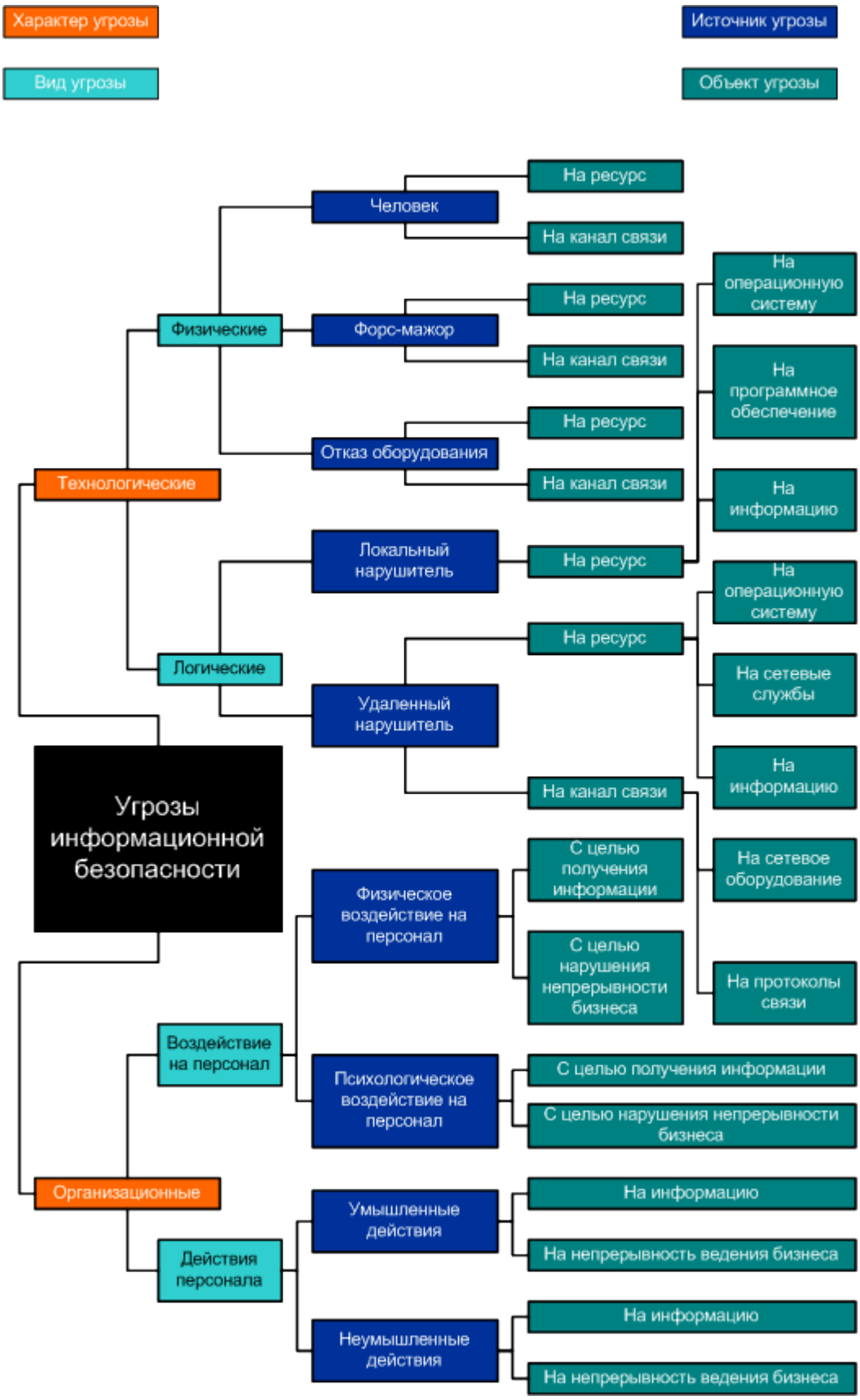
Источники угроз информационной безопасности



Источник: «Алексинцев А.И. «Безопасность информационных технологий» - 2001г. - №3».

Таблица 3

Угрозы информационной безопасности



Р Источник: «Алексинцев А.И. «Безопасность информационных технологий» - 2001г. - №3».