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.

Объектом изучения данной курсовой работы является информационная безопасность. В связи с этим, основной целью данной работы является попытка собрать необходимую информацию о существующих угрозах информационной безопасности, методах и средствах борьбы с ними, входящих в предметную область изучаемого объекта.

Задача данной работы – определить сущность информационной безопасности, определить угрозы и их составы, так же охарактеризовать основные виды угроз, рассмотреть существующие методы и средства защиты информации.

Информационной базой курсовой работы являются учебники, учебные пособия, литературные издания по соответствующей теме, статьи журналов.

Глава 1. Понятие и структура угроз защищаемой информации

1.1. Источники, виды и способы дестабилизирующего воздействия

Существует три разных подхода к выявлению угроз, которые включают следующее:

1. Угроза рассматривается как потенциально существующая ситуация (возможность, опасность) нарушения информационной безопасности, а безопасность информации означает, что информация находится в такой защищенной форме, что она способна противостоять любым дестабилизирующим эффектам;

2. Угроза рассматривается как явление (событие или возможность их возникновения), что может привести к нежелательным последствиям для информации;

3. Угроза определяется как реальные или потенциально возможные действия или условия, которые приводят к той или иной форме уязвимости информации.

Любая угроза не сводится к чему-то однозначному, она состоит из определенных взаимосвязанных компонентов, каждая из которых сама по себе не представляет угрозы, а является ее частью. Сама угроза возникает только при их совместном взаимодействии.

Угрозы защищенной информации связаны с ее уязвимостью, то есть с неспособностью информации самостоятельно противостоять дестабилизирующим влияниям, которые нарушают ее статус. Нарушение статуса защищенной информации заключается в нарушении ее физической безопасности, логической структуры и контента, доступности для приемлемых пользователей, конфиденциальности (закрытой для аутсайдеров) и выражается посредством внедрения шести форм уязвимости информации.[1]

Прежде всего, угроза должна иметь некоторые существенные проявления, и любое проявление обычно называют явлением, поэтому одним из признаков и в то же время одной из составляющих угроз должно быть явление.

В основе любого явления лежат составные причины, которые являются его движущей силой и которые, в свою очередь, обусловлены определенными обстоятельствами или предпосылками. Эти причины и обстоятельства относятся к факторам, которые создают возможность дестабилизирующего воздействия на информацию. Таким образом, факторы являются его одним знаком и компонентом угрозы.

Другим конкретным признаком угрозы является ее фокус, то есть результат, которому может привести дестабилизирующий эффект на информацию.

Угроза защищенной информации представляет собой сочетание явлений, факторов и условий, которые создают опасность нарушения статуса информации.

Чтобы выявить структуру угроз, необходимо существенно указать признаки угроз, которые, в свою очередь, должны выявить характер явлений и факторов, а также определить состав условий.

К существенным проявлениям угрозы относятся:

1. источник дестабилизирующего влияния на информацию (от кого или от чего берутся эти эффекты);

2. виды дестабилизирующего воздействия на информацию (как);

3. способы дестабилизирующего влияния на информацию (какие методы, действия выполняются и реализуются типы дестабилизирующих эффектов).

Факторы, помимо причин и обстоятельств, включают наличие каналов и методов несанкционированного доступа к конфиденциальной информации для воздействия на информацию лиц, которые не имеют к ней доступа.

Источниками дестабилизирующего воздействия на информацию являются:

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.

Наиболее распространенным, разнообразным и опасным источником дестабилизирующего влияния на защищенную информацию являются люди. Это так, потому что воздействие на защищенную информацию может обеспечить различные категории людей, как работающих, так и неработающих на предприятии.

Этот источник включает:

а) сотрудники предприятия;

б) лица, которые не работают на предприятии, но имеют доступ к защищенной информации в связи с их официальным положением;

в) сотрудники государственных разведывательных служб других стран и конкурирующих предприятий;

г) лица из криминальных структур.

Технические средства являются вторым по значимости источником дестабилизирующего воздействия на охраняемую информацию из-за их разнообразия.

Этот источник включает:

а) компьютерные технологии;

б) электрические и автоматические пишущие машинки и копировальные аппараты;

в) видео- и звукозаписывающее и воспроизводящее оборудование;

г) телефон, телеграф, громкоговоритель;

д) средства вещания и телевидения;

е) средства кабельной и радиосвязи.

Третий источник дестабилизирующего влияния на информацию включает в себя системы электроснабжения, водоснабжения, теплоснабжения, кондиционирования воздуха. К этому источнику примыкают вспомогательные электрические и радиоэлектронные системы и средства.[2]

Четвертый источник включает технологические процессы для обработки различных ядерных энергетических установок, химической промышленности, радиоэлектроники, а также объекты для производства определенных видов оружия и военной техники, которые изменяют естественную структуру окружающей среды.

Пятый источник - естественное явление, которое включает в себя два компонента:

а) стихийные бедствия;

б) атмосферные явления.

С человеческой стороны возможны следующие типы дестабилизирующих эффектов:

1. прямое воздействие на средства массовой информации защищенной информации;

2. несанкционированное распространение конфиденциальной информации;

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

4. отключение технических средств и средств связи;

5. отказ и нарушение режима работы систем для обеспечения функционирования указанных средств.

Методы прямого воздействия на носители защищенной информации могут быть следующими:

а) физическое уничтожение носителя информации;

б) создание аварийных ситуаций для перевозчиков;

в) удаление информации из средств массовой информации;

г) создание искусственных магнитных полей для размагничивания носителей;

д) введение фальсифицированной информации.

Несанкционированное распространение конфиденциальной информации может осуществляться следующим образом:

а) словесное сообщение информации;

б) передача копий носителя информации;

в) отображение носителей информации;

г) ввод информации в компьютерные сети и системы;

д) публикация информации в открытой прессе;

е) использование информации в открытых публичных выступлениях;

ж) несанкционированное распространение информации также может быть вызвано потерей носителей информации.

Способы нарушения работы технических средств и информации об обработке могут быть следующими:

а) ущерб отдельным элементам средств;

б) нарушение правил использования средств;

в) внесение изменений в порядок обработки информации;

г) заражение программ обработкой информации вредоносными программами;

д) выдача неправильных инструкций программы;

е) превышение предполагаемого количества запросов;

ж) помехи в радиоэфире с помощью дополнительного звука или фона шума, изменения (перекрытия) частот передачи информации;

з) передача ложных сигналов

и) подключение подавляющих фильтров к информационным схемам, силовым цепям и заземлению

й) нарушение режима работы систем для обеспечения функционирования фондов

К четвертому типу могут быть назначены следующие методы:

а) неправильная установка технического оборудования;

б) уничтожение (разбивка) средств, в том числе повреждение линий кабельной связи;

в) создание чрезвычайных ситуаций для технических средств;

г) отключение средств от сетей электроснабжения;

д) отказ или нарушение режима работы систем для обеспечения функционирования объектов;

е) монтаж в электронных компьютерах, разрушающих радио и закладки программ.

Способ отключения и срыва режима работы систем для обеспечения функционирования технических средств может включать:

а) неправильная установка систем;

б) разрушение систем или их отдельных элементов;

в) создание аварийных ситуаций для систем;

г) отсоединение систем от источников питания;

д) нарушение правил эксплуатации систем.

Типы дестабилизирующего эффекта второго источника:

а) отток средств;

б) сбои в работе фондов;

в) создание электромагнитного излучения;

Основными способами дестабилизирующего влияния второго источника являются:

а) технические сбои и несчастные случаи;

б) воспламенение технических средств;

в) неспособность систем обеспечить функционирование фондов;

г) отрицательные эффекты природных явлений;

д) влияние измененной структуры окружающего магнитного поля;

е) влияние вредоносных программных продуктов;

ж) уничтожение или повреждение носителя информации;

з) возникновение технических неисправностей элементов средств.

Третий источник дестабилизирующего воздействия на информацию:

а) отказ систем;

б) сбои в работе системы.

Методы этого вида включают:

а) поломки и несчастные случаи;

б) пожары;

в) отказ источников энергии;

г) влияние природных явлений;

д) возникновение технических неисправностей элементов системы;

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

ж) изменения в химическом составе окружающей среды (на объектах химической промышленности);

з) изменения локальной структуры магнитного поля в связи с деятельностью радиоэлектронных объектов и в производстве отдельных видов оружия и военной техники.

К стихийным бедствиям и в то же время типы воздействия должны включать землетрясения, наводнения, ураган (торнадо), оползни, лавины, извержения вулканов.

Атмосферные явления (типы воздействия) включают: грозу, дождь, снег, град, мороз, тепло, изменения влажности воздуха и магнитных бурь.[3]

1.2. 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]

Глава 2. Виды угроз информационной безопасности Российской Федерации

2.1. Источники угроз информационной безопасности Российской Федерации

В своей общей ориентации угрозы информационной безопасности Российской Федерации подразделяются на следующие типы:

1. угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуального, группового и общественного сознания, духовного возрождения России;

2. угрозы информационной поддержке государственной политики Российской Федерации;

3. Угрозы развитию отечественной информационной индустрии, включая промышленность информационных, телекоммуникационных и коммуникационных объектов, для удовлетворения потребностей внутреннего рынка своей продукции и вывода этих продуктов на мировой рынок и обеспечения накопления, сохранение и эффективное использование внутренних информационных ресурсов;

4. угрозы безопасности информационных и телекоммуникационных объектов и систем, которые уже развернуты и созданы в России.[5]

Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуального, группового и общественного сознания, духовного возрождения России могут быть:

1. принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, нарушающих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

2. создание монополий для формирования, получения и распространения информации в Российской Федерации, в том числе использования телекоммуникационных систем;

3. противодействие, в том числе от криминальных структур, осуществление гражданами их конституционных прав на личную и семейную тайну, тайну переписки, телефонные разговоры и другие сообщения;

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

5. незаконное использование специальных средств воздействия на индивидуальное, групповое и общественное сознание;

6. неспособность федеральных властей, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций и граждан соблюдать требования федерального законодательства, регулирующего отношения в информационной сфере;

7. Незаконное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, открытию архивных материалов, другой открытой социально значимой информации;

8. дезорганизация и уничтожение системы накопления и сохранения культурных ценностей, в том числе архивов;

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

10. вытеснение российских информационных агентств и средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от иностранных информационных структур;

11. девальвация духовных ценностей, распространение образцов массовой культуры, основанных на культе насилия, на духовные и моральные ценности, которые противоречат ценностям, принятым в российском обществе;

12. Снижение духовного, морального и творческого потенциала населения России, что значительно усложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных технологий;

13. манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационной поддержки государственной политики Российской Федерации могут быть:

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

2. блокирование деятельности государственных СМИ в информировании российской и зарубежной аудитории;

3. Низкая эффективность информационного обеспечения государственной политики Российской Федерации из-за нехватки квалифицированного персонала, отсутствия системы формирования и реализации государственной информационной политики.

Угрозы развитию отечественной информационной индустрии, в том числе индустрии информационных технологий, телекоммуникаций и коммуникаций, для удовлетворения потребностей внутреннего рынка в своих продуктах и вывода этих продуктов на мировой рынок, а также для обеспечения накопления, сохранения и эффективное использование внутренних информационных ресурсов может быть:

1. Противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и справедливому участию российских производителей в мировом разделении труда в сфере информационных услуг, информационных, телекоммуникационных и коммуникационных средствах, информационных продуктах, а также создании условий для повышения технологической зависимости России в современных информационных технологиях;

2. покупка государственными органами импортируемых средств информатизации, телекоммуникаций и связи в присутствии отечественных аналогов, не уступающих по своим характеристикам иностранным моделям;

3. вытеснение с внутреннего рынка российских производителей информационных технологий, телекоммуникаций и связи;

4. Увеличение оттока специалистов и владельцев интеллектуальной собственности за рубежом.

Угрозы безопасности информационных и телекоммуникационных объектов и систем, которые уже развернуты и созданы в России, могут быть следующими:

1. незаконный сбор и использование информации;

2. нарушения технологии обработки информации;

3. Введение в аппаратные и программные продукты компонентов, которые реализуют функции, не предусмотренные в документации для этих продуктов;

4. разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, включая системы информационной безопасности;

5. уничтожение, повреждение, электронное подавление или уничтожение средств и систем обработки информации, телекоммуникаций и связи;

6. Влияние на системы защиты паролей для автоматизированных систем обработки и передачи информации;

7. компрометация ключей и средств защиты криптографической информации;

8. утечка информации по техническим каналам;

9. внедрение электронных устройств для перехвата информации в технических средствах обработки, хранения и передачи информации по каналам связи, а также в офисах государственных органов, предприятий, учреждений и организаций независимо от формы собственности;

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

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

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

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

14. Нарушение правовых ограничений на распространение информации.

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

Внешние источники включают:

1. Деятельность внешнеполитических, экономических, военных, разведывательных и информационных структур, направленных против интересов Российской Федерации в информационной сфере;

2. Желание ряда стран доминировать и ущемлять интересы России в глобальном информационном пространстве, вытеснять ее с внешних и внутренних информационных рынков;

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

4. деятельность международных террористических организаций;

5. увеличение технологического разрыва ведущих мировых держав и наращивание их возможностей противодействовать созданию конкурентоспособных российских информационных технологий;

6. Деятельность космических, воздушных, морских и наземных технических и других средств (видов) иностранной разведки;

7. разработка несколькими государствами концепций информационных войн, которые предусматривают создание средств опасного влияния на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранение информации ресурсов и получения несанкционированного доступа к ним.[6]

Внутренние источники включают:

критическое состояние отечественной промышленности;

1. Неблагоприятная криминальная ситуация, сопровождаемая тенденциями в слиянии государственных и криминальных структур в информационной сфере, криминальными структурами, получающими доступ к конфиденциальной информации, усилением влияния организованной преступности на жизнь общества, снижением степени защиты законных интересы граждан, общества и государства в информационной сфере;

2. Неадекватная 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. Неадекватная разработка нормативно-правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

4. недоразвитость институтов гражданского общества и недостаточный государственный контроль над развитием информационного рынка в России;

5. Недостаточное финансирование мер 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. Неадекватная деятельность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по информированию общественности о своей деятельности, разъяснению принятых решений, формированию открытых государственных ресурсов и разработке системы гражданского доступа к ним;

9. Россия отстает от ведущих мировых стран по информатизации федеральных органов власти, органов государственной власти Российской Федерации и местного самоуправления, кредитно-финансового сектора, промышленности, сельского хозяйства, образования, здравоохранения, услуг и повседневной жизни граждан.[7]

2.2. 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.

Общее правовое пространство страны подрывается из-за несоблюдения приоритетного принципа норм Конституции Российской Федерации в отношении других правовых норм, федеральных правовых норм над нормами субъектов Российской Федерации и недостаточная государственная администрация на различных уровнях.

Особенно остро стоит угроза криминализации социальных отношений, сложившаяся в процессе реформирования социально-политической структуры и экономической деятельности. Серьезные просчеты на начальном этапе реформ в экономической, военной, правоохранительной и других сферах государственной деятельности, ослабление системы государственного регулирования и контроля,

несовершенство правовой базы и отсутствие сильной государственной политики в социальной сферы, снижение духовного и морального 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 слиянии определенных элементов исполнительной и законодательной ветвей с криминальными структурами, их проникновении в сферу управления банковским бизнесом, крупномасштабных производства, торговых организаций и распределительных сетей. В этой связи борьба с организованной преступностью и коррупцией носит не только юридический, но и политический характер.

Масштабы терроризма и организованной преступности растут из-за часто меняющегося конфликта форм собственности, обострения борьбы за власть, основанной на групповых и этнонационалистических интересах. Отсутствие эффективной системы социального предупреждения правонарушений, недостаточная юридическая и материально-техническая поддержка деятельности по предотвращению терроризма и организованной преступности, правовой нигилизм, отток из правоохранительных органов квалифицированного персонала повышают воздействие этой угрозы на людей, общество и государство.

Угроза национальной безопасности России в социальной сфере создается глубокой стратификацией общества в узком кругу богатых и подавляющих масс малообеспеченных граждан, увеличением доли населения, живущего за чертой бедности, и увеличением в безработице.

Угроза физическому здоровью нации - кризис систем здравоохранения и социальной защиты населения, увеличение потребления алкоголя и наркотических веществ.[8]

Последствия глубокого социального кризиса - резкое снижение рождаемости и средней продолжительности жизни в стране, деформация демографического и социального состава общества, подрыв трудовых ресурсов в качестве основы для развития производства, ослабление фундаментальной ячейки общества - семьи, духовного, морального и творческого потенциала населения.

Углубление кризиса во внутренней политической, социальной и духовной сферах может привести к потере демократических завоеваний.

Основные угрозы в международной сфере обусловлены следующими факторами:

1. Стремление отдельных государств и межгосударственных объединений умалять роль существующих механизмов обеспечения международной безопасности, прежде всего Организации Объединенных Наций 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-членов Содружества Независимых Государств;

8. претензии на территорию Российской Федерации.

Угрозы национальной безопасности Российской Федерации в международной сфере проявляются в попытках других государств выступать против укрепления России как одного из центров влияния в многополярном мире, препятствовать осуществлению национальных интересов и ослаблять его позиции в Европе, на Ближнем Востоке, в Закавказье, в Центральной Азии и в Азиатско-Тихоокеанском регионе.[9]

Терроризм представляет собой серьезную угрозу национальной безопасности Российской Федерации. Международный терроризм развязал открытую кампанию по дестабилизации ситуации в России.[10]

Угрозы национальной безопасности Российской Федерации в информационной сфере растут. Серьезной опасностью является стремление ряда стран доминировать на глобальном информационном пространстве, вытеснять Россию с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, которая предусматривает создание средств

опасного влияния на информационные сферы других стран мира; нарушения нормального функционирования информационных и телекоммуникационных систем, а также безопасности информационных ресурсов, получения несанкционированного доступа к ним.

Уровень и масштаб угроз в военной сфере возрастают.

Приведенный в ранг стратегической доктрины, переход НАТО к практике силовых (военных) действий за пределами зоны ответственности блока и без санкции Совета Безопасности ООН чреват угрозой дестабилизации всей стратегической ситуации в Мир.

Растущий технологический разрыв между несколькими ведущими державами и наращивание их возможностей для создания оружия и военной техники нового поколения создают предпосылки для качественно нового этапа гонки вооружений, фундаментального изменения форм и методов ведения военных операции.

Активно действует деятельность на территории Российской Федерации иностранных спецслужб и организаций.

Усилению негативных тенденций в военной сфере способствует длительный процесс реформирования военной организации и оборонно-промышленного комплекса Российской Федерации, недостаточное финансирование национальной обороны и несовершенство нормативно-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 неприемлемом сокращении комплектования войск (сил) современным оружием, военной и специальной техники, в чрезвычайной остроте социальных проблем и ведет к ослаблению военной безопасности Российской Федерации в целом.

Угрозы национальной безопасности и интересы Российской Федерации в приграничной зоне обусловлены:

1. экономическая, демографическая и культурно-религиозная экспансия соседних государств на территорию России;

2. Увеличение активности трансграничной организованной преступности, а также иностранных террористических организаций.

Угроза ухудшения экологической ситуации в стране и истощения ее природных ресурсов напрямую зависит от состояния экономики и готовности общества реализовать глобальный характер и важность этих проблем. Для России эта угроза особенно велика из-за преобладающего развития топливно-энергетической промышленности, недоразвитости законодательной базы для защиты окружающей среды, отсутствия или ограниченного использования экологически чистых технологий и низкой экологической культуры. Существует тенденция использовать территорию России как место для переработки и захоронения материалов и веществ, опасных для окружающей среды.

В этих условиях ослабление государственного надзора, недостаточная эффективность правовых и экономических механизмов предотвращения и ликвидации чрезвычайных ситуаций повышают риск техногенных катастроф во всех сферах экономической 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.

Список использованной литературы

1. Агальцов В.П., Титов В.М. Информатика для экономистов: Учебник. – М: ИД “ФОРУМ”: ИНФРА-М, 2006.

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

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.

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

6. Коуров Л.В. Информационные технологии. – Мн.: Амалфея, 2014.

7. Семененко В.А. Информационная безопасность: Учебное пособие. – М: МГИУ, 2015.

8. Шальгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М: ДМК Пресс, 2014.

Статьи из журналов :

9. Безмалый В. Мошенничество в Интернете // Компьютер пресс. – 2008. - №10.

10. Ульянов В. Утечки конфиденциальной информации: профиль угроз // Компьютер пресс. – 2008. - №9.

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, 2014. – 192 с. ↑

7. Семененко В.А. Информационная безопасность: Учебное пособие. – М: МГИУ, 2015. – 215 с. ↑

8. Шальгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М: ДМК Пресс, 2014. – 544 с. ↑

9. Безмалый В. Мошенничество в Интернете // Компьютер пресс. – 2008. - №10. – С. 52 - 60. ↑

10. Ульянов В. Утечки конфиденциальной информации: профиль угроз // Компьютер пресс. – 2008. - №9. – С. 29 - 32. ↑