Содержание:

Введение

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

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

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

Целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

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

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

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

1. Основные понятия и структуры защищаемой информации

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;
- угроза трактуется как явление (событие, случай или возможность их возникновения), следствием которых могут быть нежелательные воздействия на информацию;
- угроза определяется как реальные или потенциально возможные действия, или условия, приводящие к той или другой форме проявления уязвимости информации.

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

Угрозы защищаемой информации связаны с её уязвимостью, то есть неспособностью информации самостоятельно противостоять дестабилизирующим воздействиям, нарушающим её статус. А нарушение статуса защищаемой информации состоит в нарушении её физической сохранности, логической структуры и содержания, доступности для правомочных пользователей, конфиденциальности (закрытости для посторонних лиц), и выражается по средствам реализации шести форм проявления уязвимости информации.

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

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

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

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

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

К сущностным проявлениям угрозы относятся: [2]

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

1.2. Источники, виды и способы дестабилизирующего воздействия

К источникам дестабилизирующего воздействия на информацию относятся:[3]

- люди;
- технические средства отображения, хранения, обработки, воспроизведения, передачи информации, средства связи;

- системы обеспечения функционирования технических средств;
- технологические процессы отдельных категорий промышленных объектов;
- природные явления.

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

К этому источнику относятся:

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

Технические средства вторыми по источником дестабилизирующего на защищаемую в силу их .

К этому источнику :

- электронно-вычислительная ;
- электрические и автоматические и копировально-множительная ;
- средства видео и и воспроизводящей техники;
- телефонной, телеграфной, , громкоговорящей;
- средства и телевидения;
- средства и радиосвязи.

Третий дестабилизирующего воздействия информацию включает электроснабжения, водоснабжения, , кондиционирования. К этому примыкают вспомогательные и радиоэлектронные системы и .

К четвертому источнику технологические процессы различных объектов энергетики, химической , радиоэлектроники, а также по изготовлению видов вооружения и техники, которые естественную структуру среды.

Пятый – это природные , которые включают в две составляющие:

- бедствия;
- атмосферные .

Со стороны возможно следующие дестабилизирующих воздействий:

- воздействие на защищаемой информации;
  - распространение конфиденциальной ;
  - нарушение режима технических средств хранения, обработки, , передачи информации, связи и технологий информации;
  - вывод строя технических и средств связи;
  - из строя и режима работы обеспечения функционирования средств.

Способами воздействия на защищаемой информации быть:

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

распространение конфиденциальной может осуществляться образом:

- словесная информации (разбалтывание);
- копий носителя ;
- показ носителей ;
- ввод информации в сети и системы;
- информации в открытой ;
- использование информации в публичных выступлениях;

нарушение работы средств и обработки могут быть:[4]

- отдельных элементов
- нарушение правил средств
- внесение в порядок обработки
- заражение программ информации вредоносными
- выдача неправильных команд
- превышение числа запросов
- помех в радио- с помощью дополнительного или шумового , изменение (наложение) передачи информации
- ложных сигналов

- подавляющих фильтров в цепи, цепи и заземления
- нарушение работы систем функционирования средств

К виду можно следующие способы:

- - монтаж технических ;
  - разрушение (поломка) , в том числе, (разрыв) кабельных связи;
  - создание ситуаций для средств;
  - отключение от сетей ;
  - вывод из или нарушения работы систем функционирования средств;
  - в электронно-вычислительную разрушающих радио и закладок.

Способом из строя и режима работы обеспечения функционирования средств можно :

- не правильный систем;
- разрушение поломка систем их отдельных ;
- создание аварийных для систем;
- систем от питания;
- нарушения эксплуатации систем.

К дестабилизирующего воздействия источника относятся:

- средств из ;
- сбои в работе ;
- создание электромагнитных ;

Основными способами воздействия второго являются:

- технические и аварии;
- возгорание средств;
- выход строя систем функционирования средств;
- воздействия природных ;
- воздействия измененной окружающего магнитного ;
- воздействия вредоносных продуктов;
- разрушение повреждение носителя ;
- возникновение технических элементов средств.

третьего источника воздействия на являются:

- выход из строя;

- в работе системы.

К этого вида :

- поломки и аварии;
- ;
- выход из источников питания;
- природных явлений;
- технических неисправностей системы;
- изменения радиационного фона среды (на ядерной энергетики);
- химического состава среды (на химической промышленности);
- локальной структуры поля происходящего деятельности объектов и при изготовлении видов вооружения и технике.

К стихийным и одновременно видам следует отнести , наводнения, ураган (), оползни, лавины, вулканов.

К атмосферным (видам воздействия) : гроза, дождь, , град, мороз, , изменения влажности и магнитные бури.

2. Источники угроз безопасности РФ

2.1. Проявления уязвимости информации

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

2.2. Угрозы информационной безопасности Российской Федерации

своей общей угрозы информационной Российской Федерации на следующие :

- угрозы конституционным и свободам человека и в области духовной и информационной деятельности, , групповому и общественному , духовному возрождению ;
- угрозы информационному государственной политики Федерации;
- угрозы отечественной индустрии , включая индустрию информатизации, телекоммуникации и , обеспечению потребностей рынка в ее и выходу этой на мировой , а также обеспечению , сохранности и эффективного отечественных информационных ;
- угрозы безопасности и телекоммуникационных средств и , как уже , так и создаваемых территории России.

конституционным правам и человека и гражданина в духовной жизни и деятельности, индивидуальному, и общественному сознанию, возрождению России являться:

- принятие органами государственной , органами государственной субъектов Российской нормативных правовых , ущемляющих конституционные и свободы граждан в духовной жизни и деятельности;
- создание на формирование, и распространение информации в Федерации, в том с использованием телекоммуникационных ;
- противодействие, в том со стороны структур, реализации своих конституционных на личную и тайну, тайну , телефонных переговоров и сообщений;
- нерациональное, ограничение доступа к необходимой информации;
- применение специальных воздействия на , групповое и общественное ;
- неисполнение федеральными государственной власти, государственной власти Российской Федерации, местного самоуправления, и гражданами требований законодательства, регулирующего в информационной сфере;
- ограничение доступа к открытым информационным федеральных органов власти, органов власти субъектов Федерации, органов самоуправления, к открытым материалам, к другой социально значимой ;
- дезорганизация и разрушение накопления и сохранения ценностей, включая ;
- нарушение конституционных и свобод человека и в области массовой ;

- вытеснение российских агентств, средств информации с внутреннего рынка и усиление духовной, экономической и сфер общественной России от информационных структур;
- духовных ценностей, образцов массовой , основанных на насилия, на и нравственных ценностях, ценностям, принятым в обществе;
- снижение , нравственного и творческого населения России, существенно осложнит трудовых ресурсов внедрения и использования технологий, в том информационных;
- манипулирование (дезинформация, сокрытие искажение информации).

информационному обеспечению политики Российской могут являться:

-
  - информационного рынка , его отдельных отечественными и зарубежными структурами;
  - блокирование государственных средств информации по российской и зарубежной ;
  - низкая эффективность обеспечения государственной Российской Федерации дефицита квалифицированных , отсутствия системы и реализации государственной политики.

Угрозами отечественной индустрии , включая индустрию информатизации, телекоммуникации и , обеспечению потребностей рынка в ее и выходу этой на мировой , а также обеспечению , сохранности и эффективного отечественных информационных могут являться:

- доступу Российской к новейшим информационным , взаимовыгодному и равноправному российских производителей в разделении труда в информационных услуг, информатизации, телекоммуникации и , информационных продуктов, а создание условий усиления технологической России в области информационных технологий;
- органами государственной импортных средств , телекоммуникации и связи наличии отечественных , не уступающих своим характеристикам образцам;
- вытеснение с рынка российских средств информатизации, и связи;
- увеличение за рубеж и правообладателей интеллектуальной .

Угрозами безопасности и телекоммуникационных средств и , как уже , так и создаваемых территории России, являться:

- противоправные и использование информации;
- технологии обработки ;

- внедрение в аппаратные и изделия компонентов, функции, не документацией на изделия;
- разработка и программ, нарушающих функционирование информационных и - телекоммуникационных систем, в числе систем информации;
- уничтожение, , радиоэлектронное подавление разрушение средств и обработки информации, и связи;
- воздействие парольно-ключевые защиты автоматизированных обработки и передачи ;
- компрометация ключей и криптографической защиты ;
- утечка информации техническим каналам;
- электронных устройств перехвата информации в средства обработки, и передачи информации каналам связи, а в служебные помещения государственной власти, , учреждений и организаций от формы ;
- уничтожение, повреждение, или хищение и других носителей ;
- перехват информации в передачи данных и линиях связи, этой информации и ложной информации;
- несертифицированных отечественных и информационных технологий, защиты информации, информатизации, телекоммуникации и при создании и российской информационной ;
- несанкционированный доступ к , находящейся в банках и данных;
- нарушение ограничений на информации.

2.3. Источники информационной безопасности РФ

Источники информационной безопасности Федерации подразделяются внешние и внутренние.

К источникам относятся:

- иностранных политических, , военных, разведывательных и структур, направленная интересов Российской в информационной сфере;
- ряда стран к и ущемлению интересов в мировом информационном , вытеснению ее с и внутреннего информационных ;
- обострение международной за обладание технологиями и ресурсами;
- международных террористических ;
- увеличение технологического ведущих держав и наращивание их по противодействию конкурентоспособных российских технологий;

- деятельность , воздушных, морских и технических и иных (видов) разведки государств;
- разработка государств концепций войн, предусматривающих средств опасного на информационные других стран , нарушение нормального информационных и телекоммуникационных , сохранности информационных , получение несанкционированного к ним.

К внутренним относятся:[6]

критическое отечественных отраслей ;

- неблагоприятная криминогенная , сопровождающаяся тенденциями государственных и криминальных в информационной сфере, криминальными структурами к конфиденциальной информации, влияния организованной на жизнь , снижения степени законных интересов , общества и государства в сфере;
- недостаточная деятельности федеральных государственной власти, государственной власти Российской Федерации формированию и реализации государственной политики в обеспечения информационной Российской Федерации;
- разработанность нормативной базы, регулирующей в информационной сфере, а недостаточная правоприменительная ;
- неразвитость институтов общества и недостаточный контроль за информационного рынка ;
- недостаточное финансирование по обеспечению безопасности Российской ;
- недостаточная экономическая государства;
- снижение системы образования и , недостаточное количество кадров в области информационной безопасности;
- активность федеральных государственной власти, государственной власти Российской Федерации в общества о своей , в разъяснении принимаемых , в формировании открытых ресурсов и развитии доступа к ним ;
- отставание России ведущих стран по уровню федеральных органов власти, органов власти субъектов Федерации и органов самоуправления, кредитно-сферы, промышленности, хозяйства, образования, , сферы услуг и граждан.

Состояние отечественной , несовершенство системы государственной власти и общества, социально- поляризация российского и криминализация общественных , рост организованной и увеличение масштабов , обострение межнациональных и международных отношений широкий спектр и внешних угроз безопасности страны.

В экономики угрозы комплексный характер и прежде всего сокращением внутреннего продукта, снижением , инновационной активности и -технического потенциала, аграрного сектора, банковской системы, внешнего и внутреннего долга, тенденцией к в экспортных поставках -сырьевой и энергетической , а в импортных поставках - и предметов потребления, предметы первой .

Ослабление научно- и технологического потенциала , сокращение исследований стратегически важных научно-технического , отток за специалистов и интеллектуальной угрожают России передовых позиций в , деградацией наукоемких , усилением внешней зависимости и подрывом России.

Негативные в экономике лежат в сепаратистских устремлений субъектов Российской . Это ведет к политической нестабильности, единого экономического России и его составляющих - производственно- и транспортных связей, - банковской, кредитной и систем.

Экономическая , социальная дифференциация , девальвация духовных способствуют усилению во взаимоотношениях и центра, представляя угрозу федеративному и социально-экономическому Российской Федерации.

, этноцентризм и шовинизм, в деятельности ряда объединений, а также миграция способствуют национализма, политического и экстремизма, этносепаратизма и условия для конфликтов.

Единое пространство страны вследствие несоблюдения приоритета норм Российской Федерации иными правовыми , федеральных правовых над нормами Российской Федерации, отлаженности государственного на различных .

Угроза криминализации отношений, складывающихся в реформирования социально- устройства и экономической , приобретает особую . Серьезные просчеты, на начальном проведения реформ в , военной, правоохранительной и областях государственной , ослабление системы регулирования и контроля, правовой базы и сильной государственной в социальной сфере, духовно-нравственного общества являются факторами, способствующими преступности, особенно организованных форм, а коррупции.

Последствия просчетов проявляются в правового контроля ситуацией в стране, в отдельных элементов и законодательной власти с структурами, проникновении в сферу управления бизнесом, крупными , торговыми организациями и сетями. В связи с борьба с организованной и коррупцией имеет только правовой, и

политический характер.

терроризма и организованной возрастают вследствие сопровождающегося конфликтами форм собственности, борьбы за на основе и этнонационалистических интересов.

эффективной системы профилактики правонарушений, правовая и материально-обеспеченность деятельности предупреждению терроризма и преступности, правовой , отток из обеспечения правопорядка кадров увеличивают воздействия этой на личность, и государство.

Угрозу безопасности России в сфере создают расслоение общества узкий круг и преобладающую массу граждан, увеличение веса населения, за чертой , рост безработицы.

физическому здоровью являются кризис здравоохранения и социальной населения, рост алкоголя и наркотических .

Последствиями глубокого кризиса являются сокращение рождаемости и продолжительности жизни в , деформация демографического и состава общества, трудовых ресурсов основы развития , ослабление фундаментальной общества - семьи, духовного, нравственного и потенциала населения.

кризиса во , социальной и духовной может привести к демократических завоеваний.

угрозы в международной обусловлены следующими :[7]

- стремление отдельных и межгосударственных объединений роль существующих обеспечения международной , прежде всего и ОБСЕ;
- опасность политического, экономического и влияния России в ;
- укрепление военно- блоков и союзов, всего расширение на восток;
- появления в непосредственной от российских иностранных военных и крупных воинских ;
- распространение оружия уничтожения и средств доставки;
- ослабление процессов в Содружестве Государств:
- возникновение и конфликтов вблизи границы Российской и внешних границ - участников Содружества Государств;
- притязания территорию Российской .

Угрозы национальной Российской Федерации в сфере проявляются в других государств укреплению России одного из влияния в многополярном , помешать реализации интересов и ослабить позиции в Европе, Ближнем Востоке, в , Центральной Азии и -Тихоокеанском регионе.

угрозу национальной Российской Федерации терроризм. Международным развязана открытая в целях дестабилизации в России.

Усиливаются национальной безопасности Федерации в информационной . Серьезную опасность собой стремление стран к доминированию в информационном пространстве, России с внешнего и информационного рынка; рядом государств информационных войн, создание средств воздействия на сферы других мира; нарушение функционирования информационных и систем, а также информационных ресурсов, несанкционированного доступа к .

Возведенный в ранг доктрины переход к практике силовых () действий вне ответственности блока и санкции Совета ООН чреват дестабилизации всей обстановки в мире.

технологический отрыв ведущих держав и их возможностей созданию вооружений и техники нового создают предпосылки нового этапа вооружений, коренного форм и способов военных действий.

деятельность на Российской Федерации специальных служб и ими организаций.

негативных тенденций в сфере способствуют процесс реформирования организации и оборонного комплекса Российской , недостаточное финансирование обороны и несовершенство правовой базы. современном этапе проявляется в критически уровне оперативной и подготовки Вооруженных Российской Федерации, войск, воинских и органов, в недопустимом укомплектованности войск () современным вооружением, и специальной техникой, в остроте социальных и приводит к ослаблению безопасности Российской в целом.

Угрозы безопасности и интересам Федерации в пограничной обусловлены:

- экономической, и культурно-религиозной сопредельных государств российскую территорию;
- деятельности трансграничной преступности, а также террористических организаций.

ухудшения экологической в стране и истощения природных ресурсов в прямой зависимости состояния экономики и общества осознать и важность этих . Для России угроза особенно из-за развития топливно- отраслей промышленности, законодательной основы деятельности, отсутствия ограниченного использования технологий, низкой культуры. Имеет тенденция к использованию России в качестве переработки и захоронения для окружающей материалов и веществ.

В условиях ослабление надзора, недостаточная правовых и экономических предупреждения и ликвидации ситуаций увеличивают катастроф техногенного во всех хозяйственной деятельности.

3. Противодействие угрозам безопасности

3.1. Основные противодействия информационным угрозам

По способам все меры информации, ее и систем ее подразделяются на:[8]

- (законодательные);
- морально-;
- технологические;
- организационные (и процедурные);
- физические;
- (аппаратурные и программные).
- (законодательные)

К правовым защиты относятся в стране законы, и другие нормативно- акты, регламентирующие обращения с информацией, права и обязанности информационных отношений в ее получения, и использования, а также ответственность за этих правил, тем самым использованию информации и сдерживающим фактором потенциальных нарушителей. меры защиты в основном упреждающий, характер и требуют разъяснительной работы с и обслуживающим персоналом .

Морально-этические:

К -этическим мерам относятся нормы , которые традиционно или складываются мере распространения технологий в обществе. нормы большей не являются , как требования актов, однако, несоблюдение ведет к падению авторитета престижа человека, лиц или . Морально-этические бывают как (например, общепризнанные честности, патриотизма и т.п.), и писаные, то оформленные в некоторый (устав, кодекс и т.п.) правил или . Морально-этические защиты являются и требуют постоянной по созданию морального климата в пользователей и обслуживающего АС.

Технологические:

К виду мер относятся разного технологические решения и , основанные обычно использовании некоторых избыточности (структурной, , информационной, временной и т.п.) и на уменьшение совершения сотрудниками и нарушений в рамках им прав и . Примером таких является использование двойного ввода информации, инициализации операций только наличии разрешений нескольких должностных , процедур проверки реквизитов исходящих и сообщении в системах сообщений, периодическое общего баланса банковских счетов и т.п.

Организацтонные:

Организационные меры - это меры и процедурного характера, процессы функционирования обработки данных, ее ресурсов, обслуживающего персонала, а порядок взаимодействия и обслуживающего персонала с таким образом, в наибольшей степени или исключить реализации угроз или снизить потерь в случае реализации.

Меры защиты:

Физические защиты основаны применении разного механических, электро-электронно-механических и сооружений, специально для создания препятствий на путях проникновения и потенциальных нарушителей к системы и защищаемой , а также средств наблюдения, связи и сигнализации. К данному относятся также и средства контроля целостности компонентов (пломбы, наклейки и т.п.).

Технические:

Технические меры основаны на различных электронных и специальных программ, в состав АС и (самостоятельно или в с другими средствами) защиты.

3.2. Достоинства различных видов защиты

Законодательные и -этические меры: [9]

меры определяют обращения с информацией и субъектов информационных за их . Законодательные и морально- меры противодействия, универсальными в том , что принципиально для всех проникновения и НСД к и информации. В некоторых они являются применимыми, как , при защите информации от тиражирования или защите от служебным положением работе с информацией.

меры:

Очевидно, в организационных структурах с уровнем правопорядка, и этики ставить о защите информации бессмысленно. Прежде надо решить и организационные вопросы. меры играют роль в обеспечении компьютерных систем. меры - это , что остается, другие методы и защиты отсутствуют не могут требуемый уровень . Однако, это не означает, систему защиты строить исключительно их основе, это часто сделать чиновники, от технического .

Этим мерам серьезные недостатки, как:

• низкая без соответствующей физическими, техническими и средствами (люди к нарушению любых дополнительных ограничений и , если только можно нарушить);

• неудобства, связанные с объемом рутинной и деятельности.

Организационные необходимы для эффективного применения мер и средств в части, касающейся действий людей. В же время меры необходимо более надежными и техническими средствами.

Физические и технические средства защиты:

Физические и технические защиты призваны недостатки организационных , поставить прочные на пути и в максимальной степени возможность неумышленных (ошибке или) нарушений регламента стороны персонала и системы.
Рассмотрим утверждение о том, создание абсолютной (есть идеально) системы защиты невозможно.
Даже допущении возможности абсолютно надежных и технических средств , перекрывающих все , которые необходимо , всегда остается воздействия на

системы, осуществляющий действия по корректного функционирования * средств (администратора , администратора безопасности и т.п.).

с самими средствами Эти люди так называемое " безопасности". В этом , стойкость системы будет определяться персонала из безопасности системы, и ее можно за счет (кадровых) мероприятий, и морально-этических .
Но даже совершенные законы и оптимальную кадровую , все равно защиты до решить не .
Во-первых, , что вряд удастся найти , в котором можно быть абсолютно , и в отношении которого было бы действий, вынуждающих нарушить запреты.
-вторых, даже надежный человек допустить случайное, нарушение.

Основные построения системы ресурсов АС:

системы обеспечения информации в АС и функционирование должны в соответствии со основными принципами:

•

• системность

• комплексность

•

• своевременность

• преемственность и совершенствования • разумная

• персональная ответственность

• функций

• минимизация

• взаимодействие и сотрудничество

• системы защиты

• алгоритмов и механизмов

• простота применения защиты

• научная и техническая реализуемость

• и профессионализм

• взаимодействие и

• обязательность контроля.

Законность:

Предполагает осуществление мероприятий и разработку безопасности информации в в соответствии с действующим в области информации, и защиты информации, нормативных актов безопасности, утвержденных государственной власти в их компетенции, с всех дозволенных обнаружения и пресечения при работе с .

Системность:

Системный к защите информации в предполагает учет взаимосвязанных, взаимодействующих и во времени , условий и факторов, значимых для и решения проблемы информационной безопасности в .

При создании защиты должны все слабые и уязвимые места обработки информации, а характер, возможные и направления атак систему со нарушителей, пути в распределенные системы и к информации. Система должна строиться с не только известных каналов и НСД к информации, и с учетом возможности принципиально новых реализации угроз .

Комплексность:

Комплексное методов и средств компьютерных систем согласованное применение средств при целостной системы , перекрывающей все (значимые) каналы угроз и не слабых мест стыках отдельных компонентов. Защита строиться эшелонировано. защита должна физическими средствами, , технологическими и правовыми . Одним из укрепленных рубежей быть средства , реализованные на операционных систем () СВТ в силу , что ОС - та часть системы, которая использованием всех ресурсов. Прикладной защиты, учитывающий предметной области, внутренний рубеж .

Непрерывность защиты:

информации - не мероприятие и не совокупность проведенных и установленных средств , а непрерывный целенаправленный , предполагающий принятие мер на этапах жизненного АС, начиная с ранних стадий , а не только этапе ее .

Большинству физических и средств защиты эффективного выполнения функций необходима организационная (административная) (своевременная смена и правильного хранения и имен, паролей, шифрования, переопределение и т.п.). Перерывы в работе защиты могут использованы злоумышленниками анализа применяемых и средств защиты, внедрения специальных и аппаратных "закладок" и средств преодоления защиты после ее функционирования.

Своевременность:

Предполагает упреждающий мер обеспечения информации, то постановку задач комплексной защите и реализацию мер безопасности информации ранних стадиях АС в целом и системы защиты , в частности.
Разработка защиты должна параллельно с разработкой и самой защищаемой . Это позволит требования безопасности проектировании архитектуры и, в счете, создать эффективные (как затратам ресурсов, и по стойкости) системы.

Преемственность и совершенствование:

Предполагают постоянное мер и средств информации на преемственности организационных и решений, кадрового , анализа функционирования и ее системы с учетом изменений в и средствах перехвата и воздействия на АС, нормативных по защите, отечественного и зарубежного в этой области.

функций:

Принцип функций, требует, ни один организации не полномочий, позволяющих единолично осуществлять критичных операций. такие операции быть разделены части, и их должно быть различным сотрудникам. того, необходимо специальные меры недопущения сговора и ответственности между сотрудниками.

Разумная (экономическая целесообразность, возможного ущерба и):

Предполагает соответствие затрат на безопасности информации информационных ресурсов возможного ущерба их разглашения, , утечки, уничтожения и .
Используемые меры и обеспечения безопасности ресурсов не заметно ухудшать показатели работы , в которой эта циркулирует. Излишние безопасности, помимо

неэффективности, приводят к и раздражению персонала.
абсолютно непреодолимую защиты принципиально . Пока информация в обращении, принимаемые могут только вероятность негативных или ущерб них, но исключить их . При достаточном времени и средств преодолеть любую . Поэтому имеет рассматривать некоторый уровень обеспечения . Высокоэффективная система стоит дорого, при работе часть ресурсов системы и может ощутимые дополнительные пользователям. Важно выбрать тот уровень защиты, котором затраты, и размер возможного были бы (задача анализа).

Персональная ответственность:

возложение ответственности обеспечение безопасности и системы ее на каждого в пределах его . В соответствии с этим распределение прав и сотрудников строится образом, чтобы в любого нарушения виновников был известен или к минимуму.

Минимизация полномочий:

Означает предоставление минимальных прав в соответствии с производственной . Доступ к информации предоставляться только в случае и объеме, в это необходимо для выполнения должностных обязанностей.

и сотрудничество:

Предполагает благоприятной атмосферы в подразделении. В такой сотрудники должны соблюдать установленные и оказывать содействие в подразделений обеспечения информации.

Гибкость защиты:

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

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

Открытость алгоритмов и механизмов защиты:

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

Простота применения средств защиты:

Механизмы зашиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Научная обоснованность и техническая реализуемость:

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

Специализация и профессионализм:

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

Взаимодействие и координация:

Предполагают осуществление мер обеспечения безопасности информации на основе взаимодействия всех заинтересованных министерств и ведомств,

предприятий и организаций при разработке и функционировании АС и ее системы защиты информации, подразделений и специалистов органов МВД специализированных предприятий и организаций в области защиты информации, привлеченных для разработки системы защиты информации в АС, координации их усилий для достижения поставленных целей Гостехкомиссией России (на этапе разработки и внедрения АС) и подразделениями безопасности органов МВД (на этапе функционирования системы).

Обязательность контроля:

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

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

Выводы:

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

Заключение

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

Самым опасным источником дестабилизирующего воздействия на информацию является человек, потому как на защищаемую информацию могут оказывать воздействие различные категории людей.

Разнообразие видов и способов дестабилизирующего воздействия на защищаемую информацию говорит о необходимости комплексной системы защиты информации.

Современная Доктрина информационной безопасности Российской Федерации наиболее полно раскрывает виды и источники угроз информационной безопасности, а также методы обеспечения информационной безопасности.

Список литературы

1. Агальцов В.П., Титов В.М. Информатика для экономистов: Учебник. – М: ИД “ФОРУМ”: ИНФРА-М, 2016. – 448 с.

2. Гаврилов М.В. Информатика и информационные технологии: Учебник. – М: Гардарики, 2016. – 655 с.

3. Домарев В.В. Безопасность информационных технологий. – К: ООО “ТИД “ДС”, 2015. – 992 с.

4. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М: Логос; ПБОЮЛ, 2015. – 264 с.

5. Компьютерные системы и сети: Учебное пособие / Под ред. В.П. Косарева и Л.В. Еремина. – М: Финансы и статистика, 2015. – 464 с.

6. Коуров Л.В. Информационные технологии. – Мн.: Амалфея, 2015. – 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, 2015. – 544 с.