Содержание:

Введение

Под информационной безопасностью понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Информационная безопасность достигается обеспечением конфиденциальности, целостности и достоверности обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов КС.

Конфиденциальность – это свойство, указывающее на необходимость введения ограничения доступа к данной информации для определенного круга лиц. Другими словами, это гарантия того, что в процессе передачи данные могут быть известны только легальным пользователям.

Целостность – это свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения в неискаженном виде по отношению к некоторому фиксированному состоянию. Информацию может создавать, изменять или уничтожать только авторизованное лицо (законный, имеющий право доступа пользователь).

Достоверность – это свойство информации, выражающееся в строгой принадлежности субъекту, который является ее источником, либо тому субъекту, от которого эта информация принята.

Доступность – это свойство информации, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к необходимой информации.

Информационная безопасность достигается проведением руководством соответствующего уровня политики информационной безопасности. Основным документом, на основе которого проводится политика информационной безопасности, является программа информационной безопасности. Этот документ разрабатывается как официальный руководящий документ высшими органами управления государством, ведомством, организацией. В документе приводятся

цели политики информационной безопасности и основные направления решения задач защиты информации в КС. В программах информационной безопасности содержатся также общие требования и принцип построения систем защиты информации в КС.

Для того чтобы обеспечить эффективную защиту информации, необходимо в первую очередь рассмотреть и проанализировать все факторы, представляющие угрозу информационной безопасности.

Глава 1. Классификация угроз информационной безопасности

Под угрозой информационной безопасности КС обычно понимают потенциально возможное событие, действие, процесс или явление, которое может оказать нежелательное воздействие на систему и информацию, которая в ней хранится и обрабатывается. Такие угрозы, воздействуя на информацию через компоненты КС, могут привести к уничтожению, искажению, копированию, несанкционированному распространению информации, к ограничению или блокированию доступа к ней. В настоящее время известен достаточно обширный перечень угроз, который классифицируют по нескольким признака.

- 1. **Природа возникновения. Естественные и искусственные угрозы**

К **естественным угрозам** относятся пожары, наводнения, ураганы, удары молний и другие стихийные бедствия и явления, которые не зависят от человека. Наиболее частыми среди этих угроз являются пожары. Для обеспечения безопасности информации, необходимым условием является оборудование помещений, в которых находятся элементы системы (носители цифровых данных, серверы, архивы и пр.), противопожарными датчиками, назначение ответственных за противопожарную безопасность и наличие средств пожаротушения. Соблюдение всех этих правил позволит свести к минимуму угрозу потери информации от пожара.

Если помещения с носителями ценной информации располагаются в непосредственной близости от водоемов, то они подвержены угрозе потери информации вследствие наводнения. Единственное что можно предпринять в данной ситуации - это исключить хранение носителей информации на первых этажах здания, которые подвержены затоплению.

Еще одной естественной угрозой являются молнии. Очень часто при ударах молнии выходят из строя сетевые карты, электрические подстанции и другие устройства. Особенно ощутимые потери, при выходе сетевого оборудования из строя, несут крупные организации и предприятия, такие как банки. Во избежание подобных проблем необходимо соединительные сетевые кабели были экранированы (экранированный сетевой кабель устойчив к электромагнитным помехам), а экран кабеля следует заземлить. Для предотвращения попадания молнии в электрические подстанции, следует устанавливать заземленный громоотвод, а компьютеры и серверы комплектовать источниками бесперебойного питания.

Следующим видом угроз являются **искусственные угрозы**, которые в свою очередь, **делятся на непреднамеренные и преднамеренные угрозы. Непреднамеренные угрозы** - это действия, которые совершают люди по неосторожности, незнанию, невнимательности или из любопытства. К такому типу угроз относят установку программных продуктов, которые не входят в список необходимых для работы, и в последствии могут стать причиной нестабильной работы системы и потеря информации. Сюда же можно отнести и другие «эксперименты», которые не являлись злым умыслом, а люди, совершавшие их, не осознавали последствий. К сожалению, этот вид угроз очень трудно поддается контролю, мало того, чтобы персонал был квалифицирован, необходимо чтобы каждый человек осознавал риск, который возникает при его несанкционированных действиях.

Основные непреднамеренные искусственные угрозы (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

1. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т. п.);
2. неправомерное включение оборудования или изменение режимов работы устройств и программ;
3. неумышленная, порча носителей информации;
4. запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т. п.);

5. нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
6. заражение компьютера вирусами;
7. неосторожные действия, приводящие к разглашению конфиденциальной информации или делающие ее общедоступной;
8. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т. п.).
9. проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ с возможностями, представляющими угрозу для работоспособности системы и безопасности информации;
10. игнорирование организационных ограничений (установленных правил) при ранге в системе;
11. вход в систему в обход средств зашиты (загрузка посторонней операционной системы со сменных магнитных носителей и т. п.);
12. некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
13. пересылка данных по ошибочному адресу абонента (устройства);
14. ввод ошибочных данных;
15. неумышленное повреждение каналов связи.

Основные преднамеренные искусственные угрозы характеризуются возможными путями умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

1. физическое разрушение системы (путем взрыва, поджога и т. п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т. п.);
2. отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т. п.);
3. действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т. п.);

4. внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);
5. вербовка (путем подкупа, шантажа и т. п.) персонала или отдельных пользователей, имеющих определенные полномочия;
6. применение подслушивающих устройств, дистанционная фото- и видеосъемка и т. п.;
7. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводка активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т. п.);
8. перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
9. хищение носителей информации (дисков, флеш-клент, микросхем памяти, запоминающих устройств и персональных ЭВМ);
10. несанкционированное копирование носителей информации;
11. хищение производственных отходов (распечаток, записей, списанных носителей информации и т. п.);
12. чтение остатков информации из оперативной памяти и с внешних запоминающих устройств;
13. чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме, используя недостатки мультизадачных операционных систем и систем программирования;
14. незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, имитации интерфейса системы и т. п.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);
15. несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие, как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т. п.;
16. вскрытие шифров криптозащиты информации;
17. внедрение аппаратных спецвложений, программ «закладок» и «вирусов» («троянских коней» и «жучков»), т. е. таких участков программ, которые не нужны для осуществления заявленных функций, но позволяют преодолеть

систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;

18. незаконное подключение к линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;
19. незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

1. **Характер воздействия.**

Преднамеренные угрозы - угрозы, связанные со злым умыслом преднамеренного физического разрушения, впоследствии выхода из строя системы. К преднамеренным угрозам относятся внутренние и внешние атаки. Вопреки распространенному мнению, крупные компании несут многомиллионные потери зачастую не от хакерских атак, а по вине своих же собственных сотрудников. Современная история знает массу примеров преднамеренных внутренних угроз информации - это проделки конкурирующих организаций, которые внедряют или вербуют агентов для последующей дезорганизации конкурента, месть сотрудников, которые недовольны заработной платой или статусом в фирме и прочее. Для того чтобы риск таких случаев был минимален, необходимо, чтобы каждый сотрудник организации соответствовал, так называемому, «статусу благонадежности».

К внешним преднамеренным угрозам можно отнести угрозы хакерских атак. Если информационная система связана с глобальной сетью интернет, то для предотвращения хакерских атак необходимо использовать межсетевой экран (так называемый firewall), который может быть, как встроен в оборудование, так и реализован программно.

Человека, пытающегося нарушить работу информационной системы или получить несанкционированный доступ к информации, обычно называют взломщиком, а иногда «компьютерным пиратом» (хакером).

В своих противоправных действиях, направленных на овладение чужими секретами, взломщики стремятся найти такие источники конфиденциальной информации, которые бы давали им наиболее достоверную информацию в

максимальных объемах с минимальными затратами на ее получение. С помощью различного рода уловок и множества приемов и средств подбираются пути и подходы к таким источникам. В данном случае под источником информации подразумевается материальный объект, обладающий определенными сведениями, представляющими конкретный интерес для злоумышленников или конкурентов.

- 1. **Цель воздействия**

По результатам акции:

1. угроза утечки;
2. угроза модификации;
3. угроза утраты.

По нарушению свойств информации:

1. угроза нарушения конфиденциальности обрабатываемой информации;
2. угроза нарушения целостности обрабатываемой информации;
3. угроза нарушения работоспособности системы (отказ в обслуживании), т. е. угроза доступности.

По природе возникновения:

1. естественные;
2. искусственные.

Естественные угрозы — это угрозы, вызванные воздействиями на компьютерную систему и ее элементы объективных физических процессов или стихийных природных явлений.

Искусственные угрозы — это угрозы компьютерной системе, вызванные деятельностью человека. Среди них, исходя и мотивации действий, можно выделить:

1. **непреднамеренные** (неумышленные, случайные) угрозы, вызванные ошибками в проектировании компьютерной системы и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т. п.;

б) **преднамеренные** (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников). Источники угроз по отношению к информационной технологии могут быть внешними или внутренними (компоненты

самой компьютерной системы - ее аппаратура, программы, персонал).

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один способ, а их некоторую совокупность из перечисленных выше.

Глава 2. Источники угроз информационной безопасности

- 1. **2.1. 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;

ж) 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. выход из строя источников питания;
3. изменения естественного радиационного фона окружающей среды (на объектах ядерной энергетики);
4. изменения химического состава окружающей среды (на объектах химической промышленности);
5. 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. **2.2. Внутренние и внешние угрозы ИБ**

К **внутренним источникам** угроз информационной безопасности относятся:

1. деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов РФ 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; увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
5. деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
6. 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:

1. критическое состояние отечественных отраслей промышленности;
2. 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;
3. недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов РФ по формированию и реализации единой государственной политики в области обеспечения информационной безопасности РФ;
4. недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
5. неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
6. недостаточное финансирование мероприятий по обеспечению ин формационной безопасности РФ;
7. недостаточная экономическая мощь государства;
8. снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
9. недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов РФ в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
10. отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан

1. **2.3. Антропогенные источники угроз**

Антропогенные источники угроз ИБ представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта (нарушителя) всегда можно оценить, спрогнозировать и принять адекватные меры.

Методы противодействия в этом случае управляемы и напрямую зависят от воли и желания организаторов защиты информации.

К антропогенным источникам угроз относятся субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления.

Субъекты (источники), действия которых могут привести к нарушению безопасности информации могут быть как внешние, так и внутренние.

Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления. Только в этом случае можно говорит о причинении ущерба. Эта группа наиболее обширна и представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия в этом случае управляемы и напрямую зависят от воли организаторов защиты информации.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению безопасности информации могут быть как внешние, так и внутренние.

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

1. криминальные структуры;
2. потенциальные преступники и хакеры;
3. недобросовестные партнеры;
4. технический персонал поставщиков телематических услуг;
5. представители надзорных организаций и аварийных служб;
6. представители силовых структур.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации

программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой, основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

1. основной персонал (пользователи, программисты, разработчики);
2. представители службы защиты информации;
3. вспомогательный персонал (уборщики, охрана);
4. технический персонал (жизнеобеспечение, эксплуатация).

Необходимо учитывать также, что особую группу внутренних антропогенных источников составляют лица с нарушенной психикой и специально внедренные и завербованные агенты, которые могут быть из числа основного, вспомогательного и технического персонала, а также представителей службы защиты информации. Данная группа рассматривается в составе перечисленных выше источников угроз, но методы парирования угрозам для этой группы могут иметь свои отличия.

Квалификация антропогенных источников информации играют важную роль в оценке их влияния и учитывается при ранжировании источников угроз.

- 1. **2.4. Техногенные источники угроз**

Вторая группа содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Однако, последствия, вызванные такой деятельностью вышли из под контроля человека и существуют сами по себе. Эти источники угроз менее прогнозируемые, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данный класс источников угроз безопасности информации особенно актуален в современных условиях, так как в сложившихся условиях эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием технического парка используемого оборудования, а также отсутствием материальных средств на его обновление.

Технические средства, содержащие потенциальные угрозы безопасности информации так же могут быть внутренними:

1. некачественные технические средства обработки информации;
2. некачественные программные средства обработки информации;
3. вспомогательные средства (охраны, сигнализации, телефонии);

4. другие технические средства, применяемые в учреждении;

и внешними:

1. средства связи;
2. близко расположенные опасные производства сети инженерных коммуникации (энерго-водоснабжения, канализации);
3. транспорт.

Последствиями применения таких технических средств, напрямую влияющими на безопасность информации, могут быть:

Нарушение нормальной работы:

1. нарушение работоспособности системы обработки информации;
2. нарушение работоспособности связи и телекоммуникаций;
3. старение носителей информации и средств ее обработки;
4. нарушение установленных правил доступа;
5. электромагнитное воздействие на технические средства.

Уничтожение (разрушение):

1. программного обеспечения, ОС, СУБД;
2. средств обработки информации (броски напряжений, протечки);
3. помещений
4. информации (размагничивание, радиация, протечки и пр.);
5. персонала.

Модификация (изменение):

1. программного обеспечения, ОС, СУБД;
2. информации при передаче по каналам связи и телекоммуникациям.
    1. **2.5. Стихийные источники угроз**

Стихийные источники угроз безопасности информации объединяют обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. К непреодолимой силе [1] в законодательстве и договорной практике относят стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть и предотвратить, или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей. Такие источники угроз

совершенно не поддаются прогнозированию и поэтому меры защиты от них должны применяться всегда. Стихийные источники, составляющие потенциальные угрозы информационной безопасности, как правило, являются внешними по отношению к рассматриваемому объекту и под ними понимаются, прежде всего, природные катаклизмы:

1. пожары;
2. землетрясения;
3. наводнения;
4. ураганы;
5. другие форс-мажорные обстоятельства (кризис в экономике, политике; войны);
6. различные непредвиденные обстоятельства (на данный момент происхождения случая);
7. необъяснимые явления;
8. сложные метеокатаклизмы.

Основной и наиболее распространенный метод защиты информации и оборудования от различных стихийных бедствий состоит в хранении архивных копий информации или в размещении некоторых сетевых устройств, например, серверов баз данных, в специальных защищенных помещениях, расположенных, как правило, в других зданиях или в другом городе.

Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии в настоящее время является установка источников бесперебойного питания. Различные по своим техническим и потребительским характеристикам, подобные устройства могут обеспечить питание всей локальной сети или отдельного компьютера в течение промежутка времени, достаточного для восстановления подачи напряжения или для сохранения информации на магнитные носители. Большинство источников бесперебойного питания одновременно выполняет функции и стабилизатора напряжения, что является дополнительной защитой от скачков напряжения в сети. Многие современные сетевые устройства - серверы, концентраторы, мосты и т. д. - оснащены собственными дублированными системами электропитания.

За рубежом крупные корпорации имеют собственные аварийные электрогенераторы или резервные линии электропитания. Эти линии подключены к разным подстанциям, и при выходе из строя одной из них электроснабжение осуществляется с резервной подстанции.

Угрозы, которые невозможно предотвратить, которые являются неконтролируемыми со стороны предприятия, могут оказывать дестабилизирующее воздействие на его деятельность. Например, могут привести к нарушению коммерческих интересов организации, вплоть до нанесения ему невосполнимых экономических потерь; снижения деловой активности или способности организации выступать в качестве конкурирующей стороны на товарных рынках; лишение предприятия научно-технического приоритета в соответствующих областях его деятельности; потеря деловой репутации, вплоть до полной остановки деятельности и банкротства.

Заключение

По результатам исследований, проведенным в данной работе можно сформулировать следующие выводы, что жизнь современного общества немыслима без современных информационных технологий, в свою очередь высокая степень автоматизации порождает риск снижения безопасности (личной, информационной, государственной, и т. п.). Доступность и широкое распространение информационных технологий, ЭВМ делает их чрезвычайно уязвимыми по отношению к деструктивным воздействиям и тому есть много примеров.

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. Домарев В. В. Безопасность информационных технологий. Системный подход — К.: ООО ТИД Диа Софт, 2014. — 992 с.

2. Лапина М. А., Ревин А. Г., Лапин В. И. Информационное право. - М.: ЮНИТИ-ДАНА, 2014. – 548 с.
3. Бармен Скотт. Разработка правил информационной безопасности. - М.: Вильямс, 2012. — 208 с.
4. Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2006. — 264 с.
5. Галицкий А. В., Рябко С. Д., Шаньгин В. Ф. Защита информации в сети. - М.: ДМК Пресс, 2014. — 616 с.
6. Гафнер В.В. Информационная безопасность: учеб. пособие. – Ростов на Дону: Феникс, 2010. - 324 с.
7. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). // «Оружие и технологии», № 11, 2014. – С.15-21.
8. Лепехин А. Н. Расследование преступлений против информационной безопасности. - М.: Тесей, 2008. — 176 с.
9. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство. - М.: 2010. — 428 с.
10. Петренко С. А., Курбатов В. А. Политики информационной безопасности. — М.: Компания АйТи, 2014. — 400 с.
11. Петренко С. А. Управление информационными рисками. - М.: Компания АйТи; ДМК Пресс, 2004. — 384 с. — ISBN 5-98453-001-5.
12. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2013. — 544 с.