Содержание:

Введение

Вступление человечества в XXI век знаменуется бурным развитием информационных технологий во всех сферах общественной жизни. Информация все в большей мере становится стратегическим ресурсом государства, производительной силой и дорогим товаром. Подобно любым другим существующим товарам, информация также нуждается в своей сохранности и надежной защите.

Уязвимость информации в компьютерных системах (КС) обусловлена большой концентрацией вычислительных ресурсов, их

территориальной рассредоточенностью, долговременным хранением больших объемов данных, одновременным доступом к ресурсам КС многочисленных пользователей. Каждый день появляются все новые и новые угрозы (сетевые атаки, несанкционированные вмешательства в КС), поэтому острота проблемы информационной безопасности с течением времени не уменьшается, а наоборот приобретает все большую актуальность.

В предметную область информационной безопасности входят такие вопросы, как: классификация и анализ угроз

безопасности, политика информационной безопасности, средства и методы защиты информации, а также управление ими.

Проблема информационной безопасности занимает важное место, так как применение информационных технологий немыслимо без повышенного внимания к вопросам защиты информации. Противоборство государств в области информационных технологий, стремление криминальных структур противоправно использовать информационные ресурсы, необходимость обеспечения прав граждан в информационной среде,

наличие множества угроз вызывают острую необходимость обеспечения защиты информации в компьютерных системах. Ущерб от нарушения (или отсутствия) информационной безопасности может привести к крупным финансовым потерям.

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, охарактеризовать основные виды угроз, рассмотреть существующие методы и средства защиты информации.

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

Глава 1. Теоретические основы информационной безопасности

1.1 Понятие и структура угроз защищаемой информации

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

1. Угроза рассматривается как потенциально существующая ситуация (возможность, опасность) нарушения безопасности информации, при этом безопасность информации означает, что информация находится в таком

защищённом виде, который способен противостоять любым дестабилизирующим воздействиям;
2. Угроза трактуется как явление (событие, случай или возможность их возникновения), следствием которых могут быть нежелательные воздействия на информацию;
3. Угроза определяется как реальные или потенциально возможные действия, или условия, приводящие к той или другой форме проявления уязвимости информации.

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

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

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

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

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

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

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

К сущностным проявлениям угрозы относятся:

1. Источник дестабилизирующего воздействия на информацию (от кого или чего исходят эти воздействия);
2. Виды дестабилизирующего воздействия на информацию (каким образом);
3. Способы дестабилизирующего воздействия на информацию (какими приёмами, действиями осуществляются и реализуются виды дестабилизирующего воздействия).

К факторам помимо причин и обстоятельств следует отнести наличие каналов и методов несанкционированного доступа к конфиденциальной информации для воздействия на информацию со стороны лиц, не имеющих к ней разрешённого доступа.

1.2 Источники, виды и способы дестабилизирующего воздействия

К источникам дестабилизирующего воздействия на информацию относятся:

1. люди;
2. технические средства отображения, хранения, обработки, воспроизведения, передачи информации, средства связи;
3. системы обеспечения функционирования технических средств;
4. технологические процессы отдельных категорий промышленных объектов;
5. природные явления.

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

К этому источнику относятся:

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

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

К этому источнику относятся:

- электронно-вычислительная техника;
- электрические и автоматические машинки и копировально-множительная техника;
- средства видео и звукозаписывающей и воспроизводящей техники;
- средства телефонной, телеграфной, факсимильной, громкоговорящей;
- средства радиовещания и телевидения;
- 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:

- стихийные бедствия;
- 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:

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

Несанкционированное распространение конфиденциальной информации может осуществляться следующим образом:

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

Способами нарушение работы технических средств и обработки информации могут быть:

- повреждения отдельных элементов средств
- нарушение правил эксплуатации средств
- внесение изменений в порядок обработки информации
- заражение программ обработки информации вредоносными программами
- выдача неправильных программных команд
- превышение расчетного числа запросов

- создание помех в радио-эфире с помощью дополнительного звукового или шумового фона, изменение (наложение) частот передачи информации
- передача ложных сигналов
- подключение подавляющих фильтров в информационные цепи, цепи питание и заземления
- нарушение режима работы систем обеспечения функционирования средств

К четвертому виду можно отнести следующие способы:

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

- не правильный монтаж систем;
- разрушение или поломка систем или их отдельных элементов;
- создание аварийных ситуаций для систем;
- отключение систем от источников питания;
- нарушения правил эксплуатации систем.

К видам дестабилизирующего воздействия второго источника относятся:

- выход средств из строя;
- сбои в работе средств;
- создание электромагнитных излучений;

Основными способами дестабилизирующего воздействия второго источника являются:

- технические поломки и аварии;
- возгорание технических средств;
- выход из строя систем обеспечения функционирования средств;

- негативные воздействия природных явлений;
- воздействия измененной структуры окружающего магнитного поля;
- воздействия вредоносных программных продуктов;
- разрушение или повреждение носителя информации;
- возникновение технических неисправностей элементов средств.

Видами третьего источника дестабилизирующего воздействия на информацию являются:

- выход систем из строя;
- сбои в работе системы.

К способам этого вида относятся:

- поломки и аварии;
- возгорания;
- выход из строя источников питания;
- воздействия природных явлений;
- появление технических неисправностей элементов системы;
- изменения естественного радиационного фона окружающей среды (на объектах ядерной энергетики);
- изменения химического состава окружающей среды (на объектах химической промышленности);
- изменения локальной структуры магнитного поля происходящего вследствие деятельности объектов радиоэлектроники и при изготовлении некоторых видов вооружения и военной технике.

К стихийным бедствиям и одновременно видам воздействия следует отнести землетрясения, наводнения, ураган (смерч), оползни, лавины, извержения вулканов.

К атмосферным явлениям (видам воздействия) относятся: гроза, дождь, снег, град, мороз, жара, изменения влажности воздуха и магнитные бури.

1.3 Информационная безопасность: понятие и угрозы

Создание всеобщего информационного пространства и

практически повсеместное применение персональных компьютеров, и внедрение компьютерных систем породило необходимость решения комплексной проблемы защиты информации.

Под защитой информации в понимается регулярное использование средств и методов, принятие мер и осуществление мероприятий с целью системного обеспечения требуемой надежности информации, хранимой и обрабатываемой с использованием средств КС. Объектом защиты является информация, или носитель, или информационный процесс, в отношении которого необходимо

обеспечить защиту в соответствии с поставленной целью защиты информации. Защита компьютерной информации включает меры предотвращения и отслеживания несанкционированного доступа (НСД) неавторизованных лиц, неправомерного использования, повреждения, уничтожения, искажения, копирования, блокирования информации в формах и носителях, связанных именно с компьютерными средствами и технологиями хранения, обработки, передачи и доступа. Для обеспечения безопасности информации в КС требуется защита: информационных массивов, представленных на

различных машинных носителях; технических средств обработки и передачи данных; программных средств, реализующих соответствующие методы, алгоритмы и технологию обработки информации; пользователей.

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.

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.

По природе возникновения различают :

естественные угрозы, вызванные воздействиями на КС объективных физических процессов или стихийных природных явлений;

искусственные угрозы безопасности, вызванные деятельностью человека.

По степени преднамеренности проявления различают случайные и преднамеренные угрозы безопасности.

По непосредственному источнику угроз. Источниками угроз могут быть:

природная среда, например, стихийные бедствия;

человек, например, разглашение конфиденциальных данных;

санкционированные программно-аппаратные средства, например, отказ в работе операционной системы;

несанкционированные программно-аппаратные средства, например, заражение компьютера вирусами.

По положению источника угроз. Источник угроз может быть расположен:

вне контролируемой зоны КС, например, перехват данных, передаваемых по каналам связи;

в пределах контролируемой зоны КС, например, хищение распечаток, носителей информации;

непосредственно в КС, например, некорректное использование ресурсов.

По степени воздействия на КС различают:

пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании КС (угроза копирования данных);

активные угрозы, которые при воздействии вносят изменения в структуру и содержание КС (внедрение аппаратных и программных спецвложений).

По этапам доступа пользователей или программ к ресурсам КС :

угрозы, которые могут проявляться на этапе доступа к ресурсам КС;

угрозы, проявляющиеся после разрешения доступа (несанкционированное использование ресурсов).

По текущему месту расположения информации в КС:

угроза доступа к информации на внешних запоминающих устройствах (ЗУ), например, копирование данных с жесткого диска;

угроза доступа к информации в оперативной памяти (несанкционированное обращение к памяти);

угроза доступа к информации, циркулирующей в линиях связи (путем незаконного подключения).

По способу доступа к ресурсам КС:

угрозы, использующие прямой стандартный путь доступа к ресурсам с помощью незаконно полученных паролей или путем несанкционированного использования терминалов законных пользователей;

угрозы, использующие скрытый нестандартный путь доступа к ресурсам КС в обход существующих средств защиты.

По степени зависимости от активности КС различают:

угрозы, проявляющиеся независимо от активности КС (хищение носителей информации);

угрозы, проявляющиеся только в процессе обработки данных (распространение вирусов).

Все множество потенциальных угроз безопасности информации в КС может быть разделено на 2 основных класса. Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют случайными или непреднамеренными. Механизм реализации случайных угроз в целом достаточно хорошо изучен, накоплен

значительный опыт противодействия этим угрозам.

Стихийные бедствия и аварии чреваты наиболее разрушительным последствиями для КС, так как последние подвергаются физическому разрушению, информация утрачивается или доступ к ней становится невозможен.

Сбои и отказы сложных систем неизбежны. В результате сбоев и отказов нарушается работоспособность технических средств, уничтожаются и искажаются данные и программы, нарушается алгоритм работы устройств.

Ошибки при разработке КС, алгоритмические и программные ошибки приводят к последствиям, аналогичным последствиям сбоев и отказов технических средств. Кроме того, такие ошибки могут быть использованы злоумышленниками для воздействия на ресурсы КС.

В результате ошибок пользователей и обслуживающего персонала нарушение безопасности происходит в 65% случаев. Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками приводит к уничтожению, нарушению целостности и конфиденциальности информации.

Преднамеренные угрозы связаны с целенаправленными действиями нарушителя. Данный класс угроз изучен недостаточно, очень динамичен и постоянно пополняется новыми угрозами.

Методы и средства шпионажа и диверсий чаще всего используются для получения сведений о системе защиты с целью проникновения в КС, а также для хищения и уничтожения информационных ресурсов. К таким методам относят подслушивание, визуальное наблюдение, хищение документов и машинных носителей информации, хищение программ и атрибутов системы защиты, сбор и анализ отходов машинных носителей

информации, поджоги.

Несанкционированный доступ к информации (НСД) происходит обычно с использованием штатных аппаратных и программных средств КС, в результате чего нарушаются установленные правила разграничения доступа пользователей или процессов к информационным ресурсам. Под правилами разграничения доступа понимается совокупность положений, регламентирующих права доступа лиц или процессов к единицам информации. Наиболее распространенными нарушениями являются:

перехват паролей – осуществляется специально разработанными программами;

«маскарад» – выполнение каких-либо действий одним пользователем от имени другого;

незаконное использование привилегий – захват привилегий законных пользователей нарушителем.

Процесс обработки и передачи информации техническими средствами КС сопровождается электромагнитными излучениями в окружающее пространство и наведением электрических сигналов в линиях связи. Они получили названия

побочных электромагнитных излучений и наводок (ПЭМИН). С помощью специального оборудования сигналы принимаются, выделяются, усиливаются и могут либо просматриваться, либо записываться в запоминающихся устройствах (ЗУ). Электромагнитные излучения используются злоумышленниками не только для получения информации, но и для ее уничтожения.

Большую угрозу безопасности информации в КС представляет несанкционированная модификация алгоритмической, программной и технической структур системы, которая получила название «закладка». Как правило, «закладки»

внедряются в специализированные системы и используются либо для непосредственного вредительского воздействия на КС, либо для обеспечения неконтролируемого входа в систему.

Одним из основных источников угроз безопасности является использование специальных программ, получивших общее название «вредительские программы». К таким программам относятся:

«компьютерные вирусы» – небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путем создания своих копий, а при выполнении

определенных условий оказывают негативное воздействие на КС;

«черви» – программы, которые выполняются каждый раз при загрузке системы, обладающие способностью перемещаться в КС или сети и самовоспроизводить копии. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти, а затем к блокировке системы;

«троянские кони» – программы, которые имеют вид полезного приложения, а на деле выполняют вредные функции (разрушение программного обеспечения, копирование и пересылка

злоумышленнику файлов с конфиденциальной информацией и т.п.).

Кроме указанных выше угроз безопасности, существует также угроза утечки информации, которая с каждым годом становится все более значимой проблемой безопасности. Чтобы эффективно справляться с утечками, необходимо знать каким образом они происходят.

На четыре основных типа утечек приходится подавляющее большинство (84%) инцидентов, причем половина этой доли (40%) приходится на самую популярную угрозу – кражу носителей. 15%

составляет инсайд. К данной категории относятся инциденты, причиной которых стали действия сотрудников, имевших легальный доступ к информации. Например, сотрудник не имел права доступа к сведениям, но сумел обойти системы безопасности. Или инсайдер имел доступ к информации и вынес ее за пределы организации. На хакерскую атаку также приходится 15% угроз. В эту обширную группу инцидентов попадают все утечки, которые произошли вследствие внешнего вторжения. Не слишком высокая доля хакерских вторжений объясняется тем, что сами вторжения стали незаметнее. 14% составила веб-

утечка. В данную категорию попадают все утечки, связанные с публикацией конфиденциальных сведений в общедоступных местах, например, в Глобальных сетях. 9% - это бумажная утечка. По определению бумажной утечкой является любая утечка, которая произошла в результате печати конфиденциальных сведений на бумажных носителях. 7% составляют другие возможные угрозы. В данную категорию попадают инциденты, точную причину которых установить не удалось, а также утечки, о которых стало известно постфактум, после использования персональных сведений в незаконных целях.

Кроме того, в настоящее время активно развивается фишинг – технология Интернет-мошенничества, которая заключается в краже личных конфиденциальных данных, таких как пароли доступа, номера кредитных карт, банковских счетов и другой персональной информации. Фишинг (от анг. Fishing - рыбалка) расшифровывается как выуживание пароля и использует не технические недостатки КС, а легковерность пользователей Интернета. Злоумышленник закидывает в Интернет приманку и “вылавливает всех рыбок” – пользователей, которые на это клюнут.

Не зависимо от специфики конкретных видов угроз, информационная безопасность должна сохранять целостность, конфиденциальность, доступность. Угрозы нарушения целостности, конфиденциальности и доступности являются первичными. Нарушение целостности включает в себя любое умышленное изменение информации, хранящейся в КС или передаваемой из одной системы в другую. Нарушение конфиденциальности может привести к ситуации, когда информация становится известной тому, кто не располагает полномочия доступа к ней. Угроза недоступности информации возникает всякий раз,

когда в результате преднамеренных действий других пользователей или злоумышленников блокируется доступ к некоторому ресурсу КС.

Еще одним видом угроз информационной безопасности является угроза раскрытия параметров КС. В результате ее реализации не причиняется какой-либо ущерб обрабатываемой в КС информации, но при этом существенно усиливаются возможности проявления первичных угроз.

Глава 2. Методы и средства защиты информации

2.1 Общая характеристика средств и методов защиты

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

Организационные мероприятия по защите включают в себя совокупность действий по подбору и проверке персонала, участвующего в подготовке и эксплуатации программ и информации, строгое регламентирование процесса разработки и функционирования КС.

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

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

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

Суть криптографической защиты заключается в приведении

(преобразовании) информации к неявному виду с помощью специальных алгоритмов либо аппаратных средств и соответствующих кодовых ключей.

2.2 Защита информации от случайных угроз

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

Дублирование информации является одним из самых эффективных способов обеспечения целостности информации. Оно обеспечивает защиту информации, как от случайных угроз, так и от преднамеренных воздействий. Для

дублирования информации могут применяться не только несъемные носители информации или специально разработанные для этого устройства, но и обычные устройства со съемными машинными носителями. Распространенными методами дублирования данных в КС являются использование выделенных областей памяти на рабочем диске и зеркальных дисков (жесткий диск с информацией, идентичной как на рабочем диске).

Под надежностью понимается свойство системы выполнять возложенные на нее функции в определенных условиях обслуживания и эксплуатации.

Надежность КС достигается на этапах разработки, производства, эксплуатации. Важным направлением в обеспечении надежности КС является своевременное обнаружение и локализация возможных неисправностей в работе ее технических средств. Значительно сократить возможности внесения субъективных ошибок разработчиков позволяют современные технологии программирования.

Отказоустойчивость – это свойство КС сохранять работоспособность при отказах отдельных устройств, блоков, схем. Известны три основных подхода к созданию отказоустойчивых систем: простое резервирование

(использование устройств, блоков, узлов, схем, только в качестве резервных); помехоустойчивое кодирование информации (рабочая информация дополняется специальной контрольной информацией-кодом, которая позволяет определять ошибки и исправлять их); создание адаптивных систем, предполагающих сохранение работоспособного состояния КС при некотором снижении эффективности функционирования в случаях отказов элементов.

Блокировка ошибочных операций. Ошибочные операции в работе КС могут быть вызваны не только случайными отказами технических и

программных средств, но и ошибками пользователей и обслуживающего персонала. Для блокировки ошибочных действий используются технические и аппаратно-программные средства, такие как блокировочные тумблеры, предохранители, средства блокировки записи на магнитные диски и другие.

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

пользователей и персонала, анализ и совершенствование процессов взаимодействия человека и КС.

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

персонала борьбе со стихийными бедствиями и авариями, методам ликвидации их последствий.

2.3 Защита КС от несанкционированного вмешательства

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

Авторизация (санкционирование, разрешение) – процедура, по которой пользователь при входе в систему опознается и получает права доступа, разрешенные системным администратором, к вычислительным

ресурсам (компьютерам, дискам, папкам, периферийным устройствам).

Авторизация выполняется программой и включает в себя идентификацию и аутентификацию.

Идентификация – предоставление идентификатора, которым может являться несекретное имя, слово, число, для регистрации пользователя в КС. Субъект указывает имя пользователя, предъявленный идентификатор сравнивается с перечнем идентификаторов. Пользователь, у которого идентификатор зарегистрирован в системе, расценивается как правомочный (легальный).

Синонимом идентификатора является логин – набор букв и цифр, уникальный для данной системы.

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

Наиболее часто применяемыми методами авторизации являются методы, основанные на использовании паролей (секретных

последовательностей символов). Пароль можно установить на запуск программы, отдельные действия на компьютере или в сети. Кроме паролей для подтверждения подлинности могут использоваться пластиковые карточки и смарт-карты.

Администрирование – это регистрация действий пользователя в сети, включая его попытки доступа к ресурсам. Для своевременного пресечения несанкционированных действий, для контроля за соблюдением установленных правил доступа необходимо обеспечить регулярный сбор, фиксацию и выдачу по запросам сведений о всех обращениях к защищаемым

компьютерным ресурсам. Основной формой регистрации является программное ведение специальных регистрационных журналов, представляющих собой файлы на внешних носителях информации.

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

методами, затрудняющими считывание скопированной информации. Основаны на создании в процессе записи информации на соответствующие накопители таких особенностей (нестандартная разметка, форматирование, носителя

информации, установка электронного ключа), которые не позволяют считывать полученную копию на других накопителях, не входящих в состав защищаемой КС. Другими словами, эти методы направлены на обеспечение совместимости накопителей только внутри данной КС.

методами, препятствующими использованию информации. Затрудняют использование полученных копированием программ и данных. Наиболее эффективным в этом отношении средством защиты является хранение информации в преобразованном криптографическими методами виде.

Другим методом противодействия несанкционированному выполнению скопированных программ является использование блока контроля среды размещения программы. Он создается при инсталляции программы и включает характеристики среды, в которой размещается программа, а также средства сравнения этих характеристик. В качестве характеристик используются характеристики ЭВМ или носителя информации.

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

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

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

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

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

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

ревизоры – запоминают исходное состояние программ, каталогов до

заражения и периодически (или по желанию пользователя) сравнивают текущее состояние с исходным;

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

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

2.4 Криптографические методы защиты информации и межсетевые

экраны

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

Шифрование – процесс маскирования сообщений или данных с целью скрытия их содержания, ограничения доступа к содержанию других лиц. Заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов. Для шифрования используются алгоритм преобразования и ключ.

Стеганография – метод защиты компьютерных данных, передаваемых по каналам

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

Кодирование – замена смысловых конструкций исходной информации (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр. При

кодировании и обратном преобразовании используются специальные таблицы или словари, хранящиеся в секрете. Кодирование широко используется для защиты информации от искажений в каналах связи.

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

информации. Поэтому сжатые файлы подвергаются последующему шифрованию.

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

Электронная цифровая подпись (ЭЦП) представляет собой строку данных, которая зависит от некоторого

секретного параметра (ключа), известного только подписывающему лицу, и от содержания подписываемого сообщения, представленного в цифровом виде. Используется для подтверждения целостности и авторства данных, нельзя изменить документ без нарушения целостности подписи.

Для блокирования угроз, исходящих из общедоступной системы, используется специальное программное или аппаратно-программное средство, которое получило название межсетевой экран (МЭ) или fire wall. МЭ позволяет разделить общую сеть на две части или более и реализовать набор

правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Иногда сетевая защита полностью блокирует трафик снаружи внутрь, но разрешает внутренним пользователям свободно связываться с внешним миром. Обычно МЭ защищают внутреннюю сеть предприятия от вторжений из глобальной сети Интернет. Межсетевой экран выполняет четыре основные функции:

фильтрация данных на разных уровнях;

использование экранирующих агентов (proxy-серверы), которые

являются программами-посредниками и обеспечивают соединение между субъектом и объектом доступа, а затем пересылают информацию, осуществляя контроль и регистрацию;

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

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

Заключение

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

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

комплекс мер, среди которых нельзя выделить наиболее важные.

Актуальность вопросов защиты информации возрастает с каждым годом. Многие считают, что данную проблему можно решить чисто техническими мерами – установкой межсетевых экранов и антивирусных программ. Но для построения надежной защиты в первую очередь необходима информация о существующих угрозах и методах противодействия им.

Известный принцип «предупрежден, значит вооружен» работает и в сфере компьютерной безопасности: вовремя распознав угрозу можно не допустить

неприятного развития событий. Поэтому нужно соблюдать меры защиты во всех точках сети, при любой работе любых субъектов с информацией.

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

Список использованной литературы

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

Безмалый В. Мошенничество в Интернете // Компьютер пресс. – 2010. - №10. – С. 52 - 60.

Гаврилов М.В. Информатика и информационные технологии: Учебник. – М: Гардарики, 2012. – 655 с.

Домарев В.В. Безопасность информационных технологий. – К: ООО “ТИД “ДС”, 2014. – 992 с.

Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М: Логос; ПБОЮЛ, 2008. – 264 с.

Компьютерные системы и сети: Учебное пособие / Под ред. В.П. Косарева и Л.В. Еремина. – М:

Финансы и статистика, 2013. – 464 с.

Коуров Л.В. Информационные технологии. – Мн.: Амалфея, 2013. – 192 с.

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

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

Шальгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М: ДМК Пресс, 2015. – 544 с.