Содержание:

Введение

Актуальность курсовой работы состоит в том, что изучение информационной безопасности позволяет защитить данные информационных систем, а также сами информационные системы от несанкционированного доступа.

В этой работе рассматривается информационная безопасность, а также защита информации от несанкционированного доступа. Эти процессы всесторонне рассматриваются при внедрении системы безопасности. Проблема защиты информации многогранна и сложна, а также охватывает ряд важных задач. Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, компьютерных систем. [2]

Защищаемая информация является собственностью и подлежит соблюдению правовых документов и требований, которые установлены владельцем информации, которым может быть один человек, группа лиц, юридические лица и государство.

Носителем защищенной информации может быть физическое лицо, материальный объект или физический объект. Информация содержится в виде символов, сигналов и изображений, технических процессов и решений, количественных характеристик физических величин.

Существует такая вещь, как объект информации, который также нуждается в защите. Охраняемый объект информации, как информационная система, предназначен для обработки защищаемой информации.

Основными объектами обеспечения информационной безопасности:

- информационные ресурсы, что содержат конфиденциальную информацию;

- системы и объекты, которые обрабатывают конфиденциальную информацию (технические средства для приема, обработки, хранения и передачи информации (ТСПИ);

- ТСПИ в средствах обработки секретной и конфиденциальной информации.

Таким образом, объекты информационной безопасности являются источниками информации для носителей информации и получателей информации.

Целью курсовой работы определение и выполнение требований к защите информации от несанкционированного доступа.

Объектом исследования в данной курсовой работе является информационная безопасность.

Предметом исследования в этом курсовом проекте является защита информации от несанкционированного доступа.

Задачи, которые поставлены в курсовом проекте:

- уточнить понятие «открытые системы» с точки зрения обеспечения их информационной безопасности;
- изучение требований по защите информации от несанкционированного доступа;
- изучение совершенствования по защите информации от несанкционированного доступа;
- анализ методов и средств защиты информации от несанкционированного доступа.

Практическая значимость курсовой работы заключается в том, что материалы исследования можно использовать при подготовки к лекциям по предметам, посвященным безопасности и защиты информации.

1 Защита информации и информационная безопасность

1.1 Определение состава защищаемой информации

Применение вычислительных средств различных областях человеческой деятельности требует наличия мощных систем обработки и передачи данных. Их

использование позволяет людям, имеющим компьютер и модем, получить доступ к информации крупнейших библиотек и баз данных мира, оперативно выполнять сложнейшие расчеты, быстро обмениваться информацией с другими респондентами сети независимо от расстояния и страны проживания.

Однако с применением таких систем возникли проблемы, связанные с утечкой информации и ее защитой. Особенно уязвимыми являются данные, которые передаются в глобальных телекоммуникационных сетях.

При этом, несмотря на современные разработки в области защиты информации, обеспечение информационной безопасности остается в наше время чрезвычайно острой проблемой.

Определение защищаемой информации - это первый шаг на пути к построению системы защиты. То, как она будет точно осуществляться, результат зависит от функционирования системы в стадии разработки. Общий подход в том, что защита производится с учетом всей конфиденциальной информации, то есть сведений, составляющих государственную тайну (секретные сведения), сведения, составляющие коммерческую тайну и определяется собственником (владельцем) части общедоступной информации. При этом конфиденциальная информация должны быть защищена от утечки и потери, а открытая – только от потери.[5]

Часто утверждается, что любая открытая информация не может быть предметом защиты. Не все согласны с включением сведений, составляющих государственную тайну, в состав конфиденциальной информации.

Защита общественной информации всегда существовала и были сделаны записи ее на носители информации, зарегистрированы их передвижения и места хранения, т. е. созданы безопасные условия хранения. Доступность информации, не умаляет ее значения, и ценная информация должна быть защищена от потери. Эта защита не должна быть направлена на ограничение доступа к информации, то есть при этом не может быть отказано в доступе к информации, но доступ должен быть в соответствии с требованиями безопасности и в соответствии с требованиями обработки и использования (например, библиотека).

При принятии решения о классификации конкретной информации, требующей защиты, должны руководствоваться определенными критериями, т. е. знаками отличия, при которых информация может быть классифицирована как защищаемая.

Очевидно, что общее основание для классификации информации как защищаемой, определяется значением информации, так как оно определяет значение информации, которую нужно защитить. Таким образом, критерии для классификации защищаемой информации, по существу, это критерии для определения его ценности.

Что касается общественной информации, такими критериями могут быть:

- Потребность в информации для юридической поддержки компании. Это относится к документированной информации, которая регулирует статус компании, права, обязанности и ответственность ее сотрудников;
- Потребность в информации для производственной деятельности (в том числе информацию, касающуюся исследований, проектирования, инжиниринга, технологий, торговли и других областях производственной деятельности);
- Необходимость информационного обеспечения деятельности, информация, необходимая для принятия решений, а также для организации производственной деятельности и обеспечения ее функционирования;
- Потребность в информации финансовой деятельности;
- Потребность в информации для обеспечения функционирования социальной сферы;
- Потребность в информации как источник доказательства в случае конфликта;
- Важность информации как исторического источника, выявление тенденций и особенностей компании.

Эти критерии определяют необходимость того, чтобы защитить общественность от потери информации. Они также вызывают необходимость защиты от потери и конфиденциальной информации. Однако основным определяющим критерием для классификации информации в качестве конфиденциальной и защиты ее от утечки является возможность воспользоваться преимуществами использования информации из-за неизвестности ее третьим лицам. Этот критерий имеет, по крайней мере, два компонента: неопределенность информации третьим лицам и преимущества в связи с этой неопределенностью. Эти элементы взаимосвязаны и взаимозависимы, поскольку, с одной стороны, неизвестная информация для третьих лиц сама по себе не имеет значения, если не обеспечивает преимущества другой - преимущества могут быть получены только из-за этой неопределенности. Конфиденциальность является правовой формой документа и в то же время обеспечением неизвестности информации.

Преимущества использования информации, которая не известна третьим лицам, могут быть с целью получения выгоды или предотвращения вреда, в зависимости от областей и сфер деятельности, политические, военные, экономические, моральные и другие характеристики, выраженные в количественных и качественных показателях.

Определенные трудности связаны с изменениями в технологиях обработки и передачи информации. Несмотря на то, что использование современных информационных технологий дает достаточное количество преимуществ: повышение эффективности процессов управления, обработки и передачи данных и т.п., развитие сетей, их взаимная интеграция, открытость приводят к появлению качественно новых угроз, имеющих потенциальную возможность воздействовать на систему.

Сегодня новая современная технология – технология защиты информации в телекоммуникационных сетях. Защищаемая информация является собственностью и подлежит соблюдению правовых документов и требований, которые установлены владельцем информации, которым может быть один человек, группа лиц, юридические лица и государство.

Технические каналы утечки информации

Каналом утечки информации называют общий источник информации, материальный носитель или среду распространения сигнала, который несет указанную информацию, и средства получения информации от сигнала или носителя.[8]

Технический канал утечки информации состоит из конфиденциального источника информации, среды распространения и средств технической разведки (злоумышленник). Рассмотрим состав технического канала утечки информации (рис.1).

Рисунок 1 – Состав технического канала утечки информации

На вход технического канала информация подается как первичный сигнал. Первичный сигнал – носитель с информацией на выходе из источника или предыдущего канала. Источником сигнала может быть:

- объект наблюдения, что отражает электромагнитные и акустические волны;
- объект наблюдения, который излучает свои собственные (тепловые) электромагнитные волны в оптическом и радио диапазонах;
- передающее устройство для канала связи;
- закладные устройства;
- источник сигнала опасности;
- источник акустических волн, которые модулируются информацией.

Поскольку информация поступает от источника во входной канал на исходном языке, передатчик выполняет преобразование представления информации в форме, обеспечивающей ее запись на носитель информации, который должен соответствовать среде распространения. Таким образом, им выполняются следующие функции [10]:

- создается поле или электрический ток, которые передают информацию;
- производится запись информации на носитель информации;
- происходит усиление мощности сигнала (носителя информации);
- предоставляет средство передачи сигнала при распространении в данной области пространства.

Среда распространения носителя информации - часть пространства, в котором происходит перемещение носителя. Ее может характеризовать набор физических параметров, которые определяют условия для перемещения носителя информации. При описании среды распространения должны быть приняты во внимание следующие параметры:

- некоторые предметы, являющиеся физическими препятствиями для субъектов и материальных объектов;
- измерение затухания на единицу длины;
- частотные характеристики;
- тип и мощность помех для сигнала.

Приемником выполняется обратная функция передатчика. Он выполняет следующие функции:

- выбирает носитель с необходимой информацией для получателя;
- производит усиление полученного сигнала до значения, что обеспечивает съем предоставленной информации;
- снимает информацию с носителя;
- преобразовывает информацию в сигнал, доступный для получателя (человека, технического устройства), а также производит его усиление до значения, необходимого для ее безупречного восприятия.

Классифицируем технические каналы утечки информации (рис. 2).

Рисунок 2 – Виды технических каналов утечки информации

1.2 Основные типы носителей информации, подлежащей защите

Информация является предметом защиты, но защищать ее как таковую невозможно, поскольку она не существует сама по себе, а фиксируется (отображается) в определенных материальных объектах или памяти людей, которые играют роль ее носителей и составляют основной, базовый объект защиты.

Согласно ГОСТ 50922-96 «Защита информации. Основные термины и определения», носитель информации – это «физическое лицо или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов».

Для регистрации как тайной, так и так и не секретной информации, используются одни и те же носители информации.

Как правило, носители секретной и конфиденциальной информации, охраняются владельцем информации.

Носители защищенной информации могут быть классифицированы как документы, продукты (элементы), вещества и материалы, электромагнитные, тепловые, радиационные и другие излучения, акустические и другие поля и т.д.

Специальным носителем информации является лицо, чей мозг исключительно сложная система хранения и обработки информации, защищенная от внешнего мира. Свойство мозга отражать и узнать о внешнем мире, накапливает в памяти огромное количество информации. Люди являются особым объектом в качестве носителя информации. Человек имеет способность генерировать новую информацию. И в качестве носителя информации, он имеет положительные и отрицательные черты.

Положительные - без согласия субъекта-носителя никакая информация не может быть извлечена, будет защищена в памяти. Он может оценить важность информации и в соответствии с этим, обращаться с ней. Он может оценить и потребителей информации, требующей защиты, то есть знать, кому и какую информацию он может доверить.

Отрицательные - он может ошибочно принять истинность потребителя информации, что должна быть защищена или преднамеренно не сохранить информацию, доверенную ему: предательство или просто разболтать.

Наиболее распространены такие типы носителей конфиденциальной информации:

Бумага, на которой информация записывается рукописными, машинописными, электронными, типографскими и другими методами, в виде текста, графики, формул и отображается в виде символов и изображений.

Магнитные носители: жесткие диски. В этих носителях информации, информация записывается (фиксируется) с помощью магнитного хранения (запись сигналов)

магнитным устройством, и отображается в виде символов. Воспроизведением (чтением) информации также занимается магнитное устройство путем восстановления сигналов.

Магнитооптические и оптические носители (оптические диски, CD-ROM). Запись данных выполняется по лазерному лучу в магнитном поле, информация отображается в виде символов, и ее считывание (воспроизведение) также осуществляется с помощью лазерного луча.

Физические поля, в которые информация записывается путем изменения интенсивности, количественных характеристик отображаемых сигналов и электромагнитных полей и в виде изображений.

.

2 Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения и передачи информации

2.1 Объекты защиты информации и носители информации

Носителем защищенной информации может быть физическое лицо, материальный объект или физический объект. Информация содержится в виде символов, сигналов и изображений, технических процессов и решений, количественных характеристик физических величин.

Объект информации, такой как информационная система с базой данных, предназначен для обработки защищаемой информации.

Основными объектами обеспечения информационной безопасности:

- информационные ресурсы, что содержат конфиденциальную информацию;

- системы и объекты, которые обрабатывают конфиденциальную информацию (технические средства для приема, обработки, хранения и передачи информации (ТСПИ);

- ТСПИ в средствах обработки секретной и конфиденциальной информации.

Общая аббревиатура - ВТС (вспомогательных технологий и систем). Она включает в себя аппаратные средства открытой телефонии, сигнализации, радио и т.д., а также объектов, которые предназначены для обработки информации с ограниченным использованием.

Таким образом, объекты информационной безопасности являются источниками информации для носителей информации и получателей информации. Тем не менее, главная цель - это защита самой информации.

В настоящее время для обеспечения защиты информации необходимо не только создавать механизмы частной защиты, но и внедрять систематический подход, включающий взаимосвязанные меры (использование специальных технических и программных инструментов, организаций, положений, нравственных и этических контрмер и т. д.).

Защита информации должна быть систематической, которая включает в себя различные взаимосвязанные компоненты. Наиболее важными из этих компонентов являются объекты защиты, поскольку их состав зависит от методов и средств защиты.

Информация подлежит защите, но ее невозможно защитить, так как она сама по себе не является основным объектом защиты.

По ГОСТ 50922-96 «Информационная безопасность. Основные термины и определения»: «носитель информации - это отдельный или материальный объект, включая физическое поле, в котором информация отображается в виде символов, изображений, сигналов, технических решений и процессов».

Носители защищенной информации могут быть классифицированы как документы, продукты (элементы), вещества и материалы, электромагнитные, тепловые, радиационные и другие излучения, акустические и другие поля и т.д.

Специальным носителем информации является лицо, чей мозг исключительно сложная система хранения и обработки информации, защищенная от внешнего мира. Свойство мозга отражать и узнать о внешнем мире, накапливает в памяти огромное количество информации. Люди являются особым объектом в качестве носителя информации. Человек имеет способность генерировать новую информацию. И в качестве носителя информации, он имеет положительные и

отрицательные черты.

Положительные - без согласия субъекта-носителя никакая информация не может быть извлечена, будет защищена в памяти. Он может оценить важность информации в соответствии с этим, обращаться с ней. Он может оценить и потребителей информации, требующей защиты, то есть знать, кому и какую информацию он может доверить.

Отрицательные - он может ошибочно принять истинность потребителя информации, что должна быть защищена или преднамеренно не сохранить информацию, доверенную ему: предательство или просто разболтать.

Среди наиболее распространенных типов носителей конфиденциальной информации, являются следующие.

Бумага, на которой информация записывается рукописными, машинописными, электронными, типографскими и другими методами, в виде текста, графики, диаграмм, формул и т.д., и отображается в виде символов и изображений.

Магнитные носители: аудиокассеты для кассетных магнитофонов, видеокассеты для некоторых видеомагнитофонов и видеокамер; жесткие диски, дискеты, магнитные ленты для компьютеров. В этих носителях информации, информация записывается (фиксируется) с помощью магнитного хранения (запись сигналов) магнитным устройством, и отображается в виде символов. Воспроизведением (чтением) информации также занимается магнитное устройство путем восстановления сигналов.

Магнитооптические и оптические носители (оптические диски, CD-ROM). Запись данных выполняется по лазерному лучу в магнитном поле, информация отображается в виде символов, и ее считывание (воспроизведение) также осуществляется с помощью лазерного луча.

Производимая продукция (продукты). Эти продукты отвечают своему назначению, и в то же время несут информацию, которая должна быть защищена. В этом случае информация отображается в виде технических решений.

Физические поля, в которые информация записывается путем изменения интенсивности, количественных характеристик отображаемых сигналов и электромагнитных полей и в виде изображений.

2.2 Защита носителей информации от потенциальных угроз

Угроза безопасности компьютерной информационной системы (КС) - это вероятность наличия в системе некоторой информации, которая прямо или косвенно может привести к повреждению или утечке другой информации.

Угрозы информационной безопасности можно разделить на два типа:

- от природных факторов – физического воздействия природных явлений на информацию - угрозы, которые не зависят от деятельности человека;

- искусственные угрозы - угрозы, вызванные деятельностью человека и такие гораздо более опасны.

Искусственные угрозы в зависимости от их мотивов, разделены на случайные и преднамеренные (умышленные).

Случайные угрозы включают в себя:

- ошибки в проектировании КС;

- ошибки в разработке программного обеспечения КС;

- случайные отказы аппаратных КС, линий связи и энергоснабжения;

- ошибки пользователей КС;

- влияние на аппаратную часть КС физических полей других электронных устройств (несоблюдение условий их электромагнитной совместимости) и т.д.

Наиболее опасны искусственные преднамеренные угрозы из-за того, что вероятность этих угроз значительно выше, чем те, которые уже описаны.

Носители конфиденциальной информации на объектах охраны должны быть защищены, в зависимости от их вида, от несанкционированного доступа, от потери и утечки информации, содержащейся в них.

Но для того, чтобы обеспечить защиту, нужно защитить и объекты, подходы к носителям и их защита действует как защита рубежей носителей. И чем больше

эти рубежи, тем сложнее их преодолеть, тем надежнее защищены носители.

В качестве первого рубежа компании рассматривают прилегающую территорию. Некоторые предприятия по периметру устанавливают контрольно-пропускные пункты. Прилегающая территория защищена от несанкционированного входа лиц в здания предприятий и промышленные зоны. Другой объект охраны – на самом предприятии. Их защита является такой же и имеет ту же цель, что и охрана территории. Защита зданий является второй линией обороны носителей информации.

Следующая защита - области, в которых находится носитель, производится обработка носителей и обеспечивается управление и производственная деятельность с использованием носителей. К таким носителям относятся:

- Помещения защиты, в которых расположены носители информации и носители информации обрабатываются. Эти области должны быть защищены от несанкционированного доступа;

- Помещения, в котором работа с носителями происходит или в рабочее время или круглосуточно: помещения, в котором работает персонал, помещения, где проводятся закрытые мероприятия (встречи, совещания, семинары и др.), производственные помещения для производства продуктов. Эти области должны быть защищены от несанкционированного доступа, от визуального наблюдения за носителями, а также, при необходимости, от прослушивания длительных конфиденциальных разговоров. Защита работает в помещении для сотрудников в виде различных технических средств, в том числе после закрытия – сигнализация.

Другой целью защиты являются непосредственно носители. Хранилища защищены от несанкционированного доступа к информации. Их защита осуществляется ответственными хранителями посредством замков, и в нерабочее время они могут защищаться иными средствами, а именно - охранной сигнализацией.

Еще одной целью защиты должны быть:

- Средства отображения, обработки, воспроизведения и передачи конфиденциальной информации, в том числе компьютеры, которые должны быть защищены от несанкционированных соединений, побочных электромагнитных излучений, компьютерных вирусов, электронных закладок, визуального наблюдения, сбоев системы, копировальная техника должна быть защищена от визуального наблюдения и электромагнитных излучений во время обработки

информации, видео-записи и методы воспроизведения, которые требуют защиты от прослушивания, визуального наблюдения и электромагнитного излучения;

- Средства транспортировки носителей конфиденциальной информации, которые должны быть защищены от покушения на носители или их разрушения во время перевозки;

- Кабели радио и связи, радиовещания и телевидения, используемые для передачи конфиденциальной информации, которые должны быть защищены от подслушивания, выхода из строя системы, аномалий;

- Работающие системы предприятия (электричество, водоснабжение, кондиционирование и т.д.) должны быть защищены от вывода из строя при использовании средств обработки и передачи конфиденциальных разговоров, визуального наблюдения за носителями;

- Технические средства защиты информации и управления должны быть защищены от несанкционированного доступа с целью удаления их из системы.

Обслуживающий персонал и пользователи также используют носители информации. Таким образом, необходима защита от несанкционированных действий не только устройств и носителей информации, но и обслуживающего персонала и пользователей.

3 Системы защиты информации

3.1 Основные требования к защите информации от несанкционированного доступа

Защита информации от несанкционированного доступа должна быть:

- непрерывной: необходимо помешать злоумышленникам обойти защиту интересующей их информации;
- плановой: разработка каждой службой детальных планов защиты информации в сфере ее компетенции с учетом общей цели предприятия (организации);
- целенаправленной: защита того, что должно защищаться в интересах конкретной цели;
- конкретной: защита конкретных данных, объективно нуждающихся в охране, утрата которых может причинить организации определенный ущерб;
- активной: защита информации с достаточной степенью настойчивости;

- надежной: методы и формы защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым информационным объектам, независимо от формы их представления, языка выражения и вида физического носителя, на котором они закреплены;
- универсальной: канал утечки необходимо перекрывать, где бы он ни проявился, разумными и достаточными средствами, независимо от характера, формы и вида информации;
- комплексной: защита информации всеми видами и формами защиты в полном объеме.

Комплексный подход к защите информации от несанкционированного доступа исходит из того, что защита представляет собой сложную систему неразрывно взаимосвязанных и взаимозависимых процессов, каждый из которых в свою очередь имеет множество различных взаимосвязанных сторон, свойств, тенденций.

При этом система защиты информации от несанкционированного доступа должна удовлетворять определенным условиям:

- охват всего технологического комплекса информационной деятельности;
- разнообразие используемых средств, многоуровневая с иерархической последовательностью доступа;
- открытость для изменения и дополнения мер обеспечения безопасности информации;
- нестандартность, разнообразность при выборе средств защиты;
- простота в техническом обслуживании и удобство эксплуатации пользователями;
- надежность технических средств, поломка которых может быть причиной появления неконтролируемых каналов утечки информации;
- комплексность, обладание целостностью, означающей, что ни одна ее часть не может быть изъята без ущерба для всей системы.

Требования к системе защиты безопасности информации от несанкционированного доступа:

- четкое определение полномочий и прав пользователей на доступ к определенным видам информации;
- определение для пользователя минимальных полномочий, необходимых ему для выполнения порученной работы;
- минимум общих для нескольких пользователей средств защиты;

- средства учета случаев и попыток несанкционированного доступа к конфиденциальной информации;
- оценка степени конфиденциальности информации;
- контроль целостности средств защиты и немедленное реагирование на их выход из строя.

3.2 Виды обеспечения системы защиты информации от несанкционированного доступа

Система защиты информации от несанкционированного доступа должна состоять из следующего:

- правовая поддержка: нормативные документы, положения, инструкции, руководящие принципы, которые являются обязательными в рамках их деятельности;

- организационная поддержка: внедрение информационной безопасности осуществляется определенными структурными подразделениями, такими как служба безопасности документов; режим обслуживания, входа, охрана; служба защиты информации техническими средствами; информационно-аналитическая деятельность и т. д.;

- аппаратное обеспечение: использование технических средств для защиты информации от несанкционированного доступа;

- информационная поддержка: информация, данные, индикаторы, параметры, которые лежат в рамках решения проблем;

- программное обеспечение: различные информационные, бухгалтерские, статистические и расчетные программы, которые могут обеспечивать несанкционированного доступа, а также опасности различных каналов утечки и способы несанкционированного доступа к источникам конфиденциальной информации;

- математическая поддержка: математические методы использования технических средств злоумышленников, зон и стандартов необходимой защиты информации от несанкционированного доступа;

- Лингвистическая поддержка: наличие норм и правил для деятельности органов, служб, средств, реализующих функции защиты информации от несанкционированного доступа, различные методы, обеспечивающие активность

пользователей при выполнении их работы. [5]

Проблема определения требований к защите информации от несанкционированного доступа, то есть когда средства электронных вычислений стали доступными для обработки конфиденциальной информации, стоит особенно остро, поскольку существует большое количество таких каналов несанкционированного доступа к информации.

Предметом информационной безопасности является компьютерная система или автоматизированная система обработки данных (АСОД).

Компьютерная система представляет собой набор аппаратного и программного обеспечения, предназначенного для автоматического сбора, хранения, обработки, передачи и получения информации. Наряду с термином «информация» по отношению к КС часто используется термин «данные». Другое определение, что используется при защите информации - «информационные ресурсы». В соответствии с законодательством Российской Федерации «Информация, информатизация и защита информации» информация ставится в соответствии с выбранными документами и отдельными документами в информационных системах (библиотеки, архивы, фонды, данные и другие информационные системы).

Концепция КС очень широка и охватывает следующие системы:

- компьютеры всех классов и назначений;
- вычислительные системы и комплексы;
- сети (местные, региональные и глобальные).

Такой широкий спектр систем в сочетании с одним определением важен по двум причинам: во-первых, для всех этих систем основные проблемы защиты информации являются общими, и вторая - меньшие системы являются элементами больших систем. Если для защиты информации в любой системе есть свои особенности, они рассматриваются отдельно.

Предметом защиты компьютерных систем является информация. Материальной основой существования информации в КС являются электронные и электромеханические устройства (подсистемы), а также аппаратура поддержки. С помощью устройств ввода или систем передачи данных (СПД) информация попадает в компьютерную систему. Системная информация сохраняется в памяти устройства (памяти) на различных уровнях, преобразуется (обработка)

процессором (РС), и из системы выходит через устройство вывода или сеть. Как компьютерные средства носителей информации используются магнитные ленты, диски различных типов. Ранее, мультимедийные компьютеры использовали бумагу, перфокарты и перфоленты, магнитные барабаны и карты. Большинство типов компьютерных носителей являются съемными, то есть могут быть удалены с устройства и использоваться (флеш-карты) или храниться (ленточные накопители, диски) отдельно от устройств. Таким образом защита информации (информационная безопасность) в компьютерных системах касается защиты устройства (подсистем) и машин от несанкционированного доступа к носителям и воздействия на них.

Однако такое рассмотрение КС с точки зрения защиты информации является неполным. Компьютерные системы представляют собой класс человеко-машинных систем. Эти системы находятся в ведении специалистов (персонала) в интересах пользователей. Кроме того, в последние годы, пользователи имеют прямой доступ к системам. Для некоторых из КС (например, ПК), пользователи выполняют функции обслуживающего персонала.

При рассмотрении защиты автоматизированных систем целесообразно использовать четыре градации доступа к хранению, обработке и защите информационной системы, которая поможет систематизировать как возможные угрозы и меры по их нейтрализации и отражения, то есть помочь систематизировать и обобщить весь спектр защиты, связанной с информационной безопасностью. Эти уровни следующие: уровень средств записи информации, уровень взаимодействия с носителем информации, уровень информации, уровень информативности.

Эти уровни были основаны на том, что:

1. Средства обработки информации часто переносятся на материал, которым может быть бумага, гибкий диск или другой носитель;

2. Если путь информации таков, что она не может быть непосредственно восприниматься человеком, существует необходимость для преобразования данных в человеческий способ представления.

3. Информация может быть охарактеризована по способу ее представления или, что также называется языком в повседневных условиях.

4. Человек должен присутствовать, чтобы определить смысл информации, ее семантику.

На рисунке 3 представлена концептуальная модель безопасности информации.

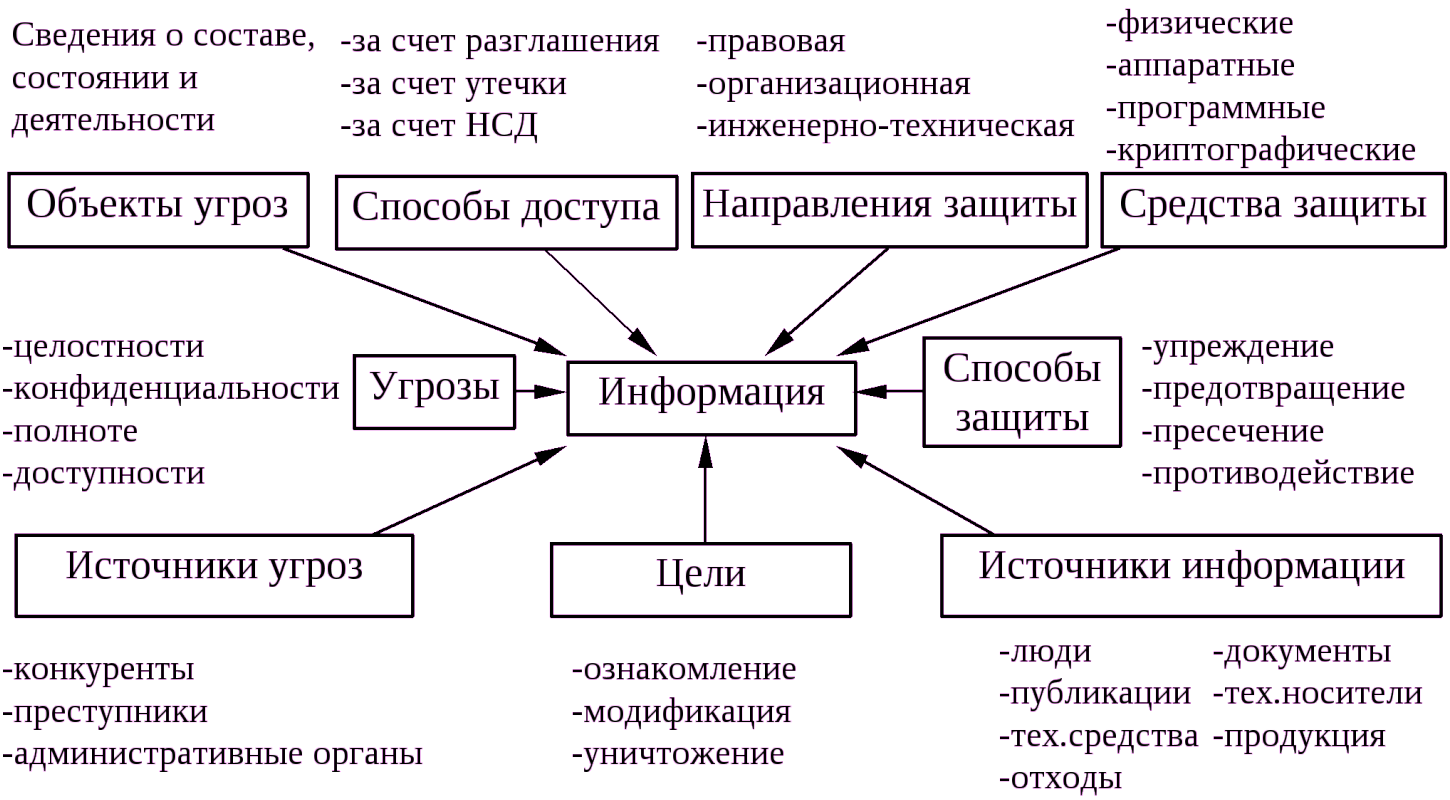

Рисунок 3 – Концептуальная модель защиты информации от несанкционированного доступа

Система защиты информации (СЗИ) в ее наиболее общей форме может быть определена как организованный набор всех средств, методов и видов деятельности, определенных в автоматизированных системах обработки данных.

К ней имеется ряд конкретных, ориентированных требований, которые можно разделить на функциональные, эргономические, экономические, технические и организационные. В комплексе эти требования показаны на рисунке 4.


ТРЕБОВАНИЯ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ
Функциональные
Обеспечение решения требуемой совокупности задач защиты
Удовлетворение всем требованиям защиты
Эргономические
Минимизация помех пользователям
Удобство для персонала системы защиты
Экономические
Минимизация затрат на систему
Максимальное использование серийных средств
Технические
Комплексное использование средств
Оптимизация архитектуры
Организационные
Структурированность всех компонентов
Простота эксплуатации

Рисунок 4 – Совокупность требований к системе защиты информации от несанкционированного доступа в АСОД.

Концептуальная единство означает, что архитектура, технологии, организация и эксплуатация СЗИ в целом и ее составных компонентов следует рассматривать и применять в строгом соответствии с основными положениями единой концепции информационной безопасности.

Адекватность требований означает, что СЗИ должны быть построены в строгом соответствии с требованиями по защите, которые в свою очередь определяются категорией безопасности соответствующего объекта, и значений параметров, влияющих на безопасность информации.

Гибкость (адаптивность) СЗИ – это построение такой организации ее функционирования, при которой функции безопасности будут осуществляться эффективно при изменении в диапазоне структуры АСОД, технологических схем, или условий эксплуатации любой из его компонентов.

Функциональная независимость подразумевает, что СЗИ должна быть вполне самостоятельной подсистемой обеспечения АСОД и при реализации функций безопасности не зависеть от других подсистем.

Удобство в использовании означает, что СЗИ не должна создавать дополнительные неудобства для пользователей и персонала АСОД.

Минимизация предоставленных прав означает, что каждый пользователь и каждый человек из персонала АСОД должны иметь ограничение в правах доступа к ресурсам АСОД в рамках только той информации, что действительно нужна для выполнения их функций в процессе автоматизированной обработки данных.

Полнота контроля требует, чтобы все процедуры автоматизированной обработки информации контролировались системой безопасности в полном объеме, и основные результаты мониторинга должны быть записаны в специальных журналах регистрации.

Активность реагирования означает, что СЗИ реагирует на любые попытки несанкционированных мероприятий и включает в себя: запрос повторить действие; задержку в выполнении запросов; отключение структурного элемента с несанкционированным действием; исключение злоумышленника из числа зарегистрированных пользователей; подача специального сигнала и т.д.

Экономичность СЗИ означает, что, при соблюдении основных требований всех предыдущих принципов расходы на СЗИ должны быть минимальны.

Требования, которые определяются автоматизированной системой обработки данных, могут быть записаны в следующем виде: информация должна быть защищена следующим образом:

- защищенная информация должна храниться только во время сеанса; в запоминающих устройствах (памяти) коммуникационного оборудования могут храниться только служебные части передаваемых сообщений;

- линии связи, по которым защищенная информация передается в ясной форме, должны быть защищены программно или аппаратно от несанкционированного доступа к передаваемой информации и находится под постоянным контролем;

- до начала каждого сеанса передачи данных, защищаемая информация должна проверяться на адреса выдачи данных;

- при передаче большого количества защищенной информации проверка адреса передачи должна осуществляться с некоторыми промежутками во времени в процессе передачи;

- если в коммуникационном оборудовании есть процессоры и память, должно вестись отслеживание и учет данных обо всех сеансах передачи защищаемой информации.

- возможность аварийного уничтожения информации при обнаружении к ней несанкционированного доступа.

Информационная безопасность достигается путем проведения руководством соответствующего уровня информационной политики безопасности. Основным документом, на основе которого проводится политика информационной безопасности, представляет собой программу информационной безопасности.

Заключение

В наше время информация имеет слишком большую ценность, чтобы можно было спокойно смотреть на ее возможную утечку. Поэтому не последнее место должна занимать организация защиты информации и необходимо целенаправленно

проводить множество мероприятий по ее защите.

Проблемы, связанные с повышением безопасности информационной сферы, являются сложными, многоплановыми и взаимосвязанными. Именно развитие информационных технологий приводит к тому, что государству и обществу необходимо постоянно прилагать совместные усилия по совершенствованию методов и средств, которые могут позволить достоверно оценивать угрозы безопасности информационной сферы и адекватно реагировать на них.

Защита информации от несанкционированного доступа предполагает использование различных средств и методов, принятие мер и осуществление мероприятий с целью полного обеспечения надежности передаваемой, хранимой и обрабатываемой информации.

Таким образом, в сфере защиты информации выделяют несколько основных задач, решение которых в информационных системах и компьютерных сетях обеспечивает необходимый уровень защиты информации:

- организация доступа к информации только допущенных к ней лиц;
- подтверждение истинности информации;
- защита от перехвата информации при передаче ее по каналам связи;
- защита от искажений и ввода ложной информации.

Защищать информацию от несанкционированного доступа – это значит:

- обеспечивать физическую целостность информации, т.е. не допускать искажений или уничтожения ее элементов;
- не допускать подмены (модификации) элементов информации при сохранении ее целостности;
- не допустить несанкционированного получения информации лицами или процессами, не имеющими на это соответствующих полномочий;
- быть уверенным в том, что передаваемые (продаваемые) владельцем информации ресурсы будут использоваться только в соответствии с обговоренными сторонами условиями.

В данной работе были выполнены следующие задачи:

- уточнено понятие «открытые системы» с точки зрения обеспечения их информационной безопасности;

- изучены требования по защите информации от несанкционированного доступа;
- изучены совершенствования по защите информации от несанкционированного доступа;
- проведен анализ методов и средств защиты информации от несанкционированного доступа.

Список использованной литературы

1. Конституция Российской Федерации.
2. Доктрина информационной безопасности России утв. Президентом РФ 9 сентября 2000 г. № Пр-1895.
3. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г. N 149-ФЗ.
4. Анализ состояния защиты данных в информационных системах: учебно-метод. пособие / В.В. Денисов. Сост.– Новосибирск: Изд-во НГТУ, 2012. – 52 с.
5. Защита от внутренних и внешних угроз информационной безопасности с помощью Info Watch Traffic Monitor и Cisco Iron Port S-Series [Электронный ресурс]. рехим доступа // http://www.infowatch.ru/sites/default/ files/patners/infowatch_traffic_monitor_ cisco_ironport_datasheet_russian.pdf
6. Ивлева А. И. Защита информации в беспроводных Wi-Fi-сетях / А. И. Ивлева. – Хабаровск: Хабаровский пограничный ин-т ФСБ России, 2014. – 142 с.: ил. – Библиогр.: с. 128-133.
7. Марков А.С., Фадин А.А. Систематика уязвимостей и дефектов безопасности программных ресурсов. // Защита информации. Инсайд. - 2013. №3. - С. 56-61.
8. Правовые аспекты использования Интернет-технологий /под ред. А.С.Кемрадж, Д.В. Головерова. – М.: Книжный мир, 2012. - 410 с.
9. Правовые основы информационной безопасности/ Ю.А. Белевская и др.; рец.: В.И. Шаров, А.С. Овчинский ; под общ. ред. А.П. Фисуна и др. - Орел: ГУ-УНПК : ОГУ, 2014. - 214 с.
10. Рабинович Е. В. Информатика для всех [Электронный ресурс]: электронный учебно-методический комплекс / Е. В. Рабинович; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://courses.edu.nstu.ru/index.php?show=155&curs=639. - Загл. с экрана.
11. Сердюк В. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий – М.: Гелиос АРВ, 2014. - 576с.

12. Сиротский А. А. Защита информации и обеспечение безопасности в беспроводных телекоммуникационных сетях // Информационные технологии. Радиоэлектроника. Телекоммуникации (ITRT - 2012): сб. ст. междунар. науч.-техн. конф. – Тольятти, 2012. – Ч. 3. – С. 256-262.
13. Топилин Я. Н. Положение о разрешительной системе допуска к информационным ресурсам организации, содержащим персональные данные (работников, клиентов, граждан) // Там же. - 2014 .- N 1 .- С. 18-24
14. Чипига А. Ф. Информационная безопасность автоматизированных систем / А. Ф. Чипига - М.: Гелиос АРВ, 2015. - 335 с.
15. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах / В. Ф. Шаньгин - М.: Форум, 2016. - 591 с.
16. Щербаков В. Б. Концептуальные основы оценки рисков и обеспечения информационной безопасности беспроводных сетей связи / В. Б. Щербаков, С. А. Ермаков // Охрана, безопасность и связь - 2016: материалы междунар. науч.-практ. конф. – Воронеж, 2016. – Ч. 2. – С. 213-216.
17. ГОСТ 50922-2006 «Защита информации. Основные термины и определения».
18. ГОСТ Р 53113.1-2008 «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения».