Объединение компьютеров в локальную сеть. Организация работы пользователей в локальных компьютерных сетях

1. Локальные компьютерные сети
2. Защита информации. Антивирусная защита

1. Локальные компьютерные сети

При работе на персональном компьютере в автономном режиме пользователи могут обмениваться информацией (программами, документами и так далее), лишь копируя ее на дискеты, диски или флэш-память.

Создание компьютерных сетей вызвано практической потребностью совместного использования информации пользователями, работающими на удаленных друг от друга компьютерах. Сети предоставляют пользователям возможность не только быстрого обмена информацией, но и совместного использования принтеров и других периферийных устройств и даже одновременной работы с документами.

Локальная сеть объединяет компьютеры, установленные в одном помещении (например, школьный компьютерный класс) или в одном здании (например, в здании школы могут быть объединены в локальную сеть несколько десятков компьютеров, установленных в различных предметных кабинетах).

Аппаратные средства локальной сети

Аппаратура локальной сети в общем случае включает в себя:

- компьютеры (серверы и рабочие станции);
- сетевые платы;
- каналы связи;
- специальные устройства, поддерживающие функционирование сети (маршрутизаторы, концентраторы, коммутаторы).

Простейшим видом локальной сети является одноранговая сеть. Из названия такой сети следует, что все компьютеры в ней имеют одинаковую значимость (статус) и ни один из них не подчинен другому.

Более развитые сети, помимо компьютеров конечных пользователей — рабочих станций, включают специальные компьютеры — серверы.

Сервер — это выделенный в сети компьютер, выполняющий функции обслуживания рабочих станций. Есть разные виды серверов: файл-серверы, серверы баз данных и др.

Каждый компьютер подключается к сети с помощью сетевой платы — адаптера, которая поддерживает конкретную схему подключения. Так, широко распространенными являются адаптеры Ethernet с пропускной способностью от 10 или 100 Мбит/с.

К сетевой плате подключается сетевой кабель. Если используется радиосвязь или связь на инфракрасных лучах, то кабель не требуется.

1. Локальные компьютерные сети

В современных локальных сетях чаще всего применяют два типа сетевых кабелей:

- неэкранированная витая пара;
- волоконно-оптический кабель.

Витая пара представляет собой набор из восьми проводов, скрученных попарно таким образом, чтобы обеспечивать защиту от электромагнитных помех. Каждая витая пара соединяет с сетью только один компьютер, поэтому нарушение соединения сказывается только на этом компьютере, что позволяет быстро находить и устранять неисправности.

Волоконно-оптические кабели передают данные в виде световых импульсов по стеклянным проводам. Большинство технологий локальных сетей в настоящее время позволяют использовать волоконно-оптические кабели. Волоконно-оптический кабель обладает существенными преимуществами по сравнению с любыми вариантами медного кабеля. Волоконно-оптические кабели обеспечивают наивысшую скорость передачи; они более надежны, так как не подвержены электромагнитным помехам. Оптический кабель очень тонок и гибок, что делает его транспортировку более удобной по сравнению с более тяжелым медным кабелем. Скорость передачи данных по оптическому кабелю составляет сотни тысяч мегабитов в секунду, что примерно в тысячу раз быстрее, чем по проводам витой пары.

Беспроводная связь на радиоволнах может использоваться для организации сетей в пределах больших помещений там, где применение обычных линий связи затруднено или нецелесообразно. Кроме того, беспроводные линии могут связывать удаленные части локальной сети на расстояниях до 25 км (при условии прямой видимости).

Совместно используемые внешние устройства включают в себя подключенные к серверу накопители внешней памяти, принтеры, графопостроители и другое оборудование, которое становится доступным с рабочих станций.

Помимо кабелей и сетевых адаптеров, в локальных сетях на витой паре используются другие сетевые устройства — концентраторы, коммутаторы и маршрутизаторы.

Концентратор (называемый также хаб) — устройство, объединяющее несколько (от 5 до 48) ветвей звездообразной локальной сети и передающее информационные пакеты во все ветви сети одинаково. Коммутатор (свич) делает то же самое, но, в отличие от концентратора, обеспечивает передачу пакетов в заданные ветви. Это обеспечивает оптимизацию потоков данных в сети и повышение защищенности от несанкционированного проникновения.

Маршрутизатор (роутер) — устройство, выполняющее пересылку данных между двумя сетями, в том числе между локальными и глобальными сетями. Маршрутизатор, по сути, является специализированным микрокомпьютером, имеет собственный процессор, оперативную и постоянную память, операционную систему.

1. Локальные компьютерные сети

Топологии сетей

Общая схема соединения компьютеров в локальной сети называется топологией сети. Топологии сети могут быть различными:

- кольцевая;
- шинная – компьютеры подключены к общему для них каналу (шине), через который могут обмениваться сообщениями;
- радиальная («звезда») – к каждому компьютеру подходит отдельный кабель из одного центрального узла;
- древовидная – иерархическая подчиненность компьютеров.

Классификация сетей по топологии.

Топология сети – это логическая схема соединения компьютеров каналами связи.

Шинная типология. Рабочие станции в любое время, без прерывания всей рабочей сети, могут быть подключены к ней или отключены. При повреждении кабеля в любом месте сети вся сеть становится неработоспособной. Достоинством шинной типологии является низкая стоимость, простота построения и наращивания сети. Недостатки – низкая скорость работы малая надёжность.

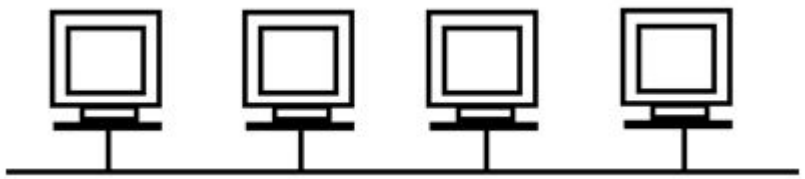

Рис.1. Структура шинной топологии вычислительной сети

1. Локальные компьютерные сети

Звездообразная типология. Этот тип типология предполагает, что головная машина получает и обрабатывает все данные с периферийных устройств. Вся информация между двумя периферийными рабочими местами через центральный узел вычислительной сети. В центре сети располагается концентратор – это устройство, обеспечивающее связь между компьютерами, входящими в сеть, т.е. все компьютеры не связываются непосредственно друг с другом, а присоединяются к концентратору. Типология в виде звезды является наиболее быстродействующей из всех типологий вычислительных сетей. Достоинством является также и то, что повреждение одного из кабелей приводит к выходу из строя только того луча «звезды», где находится повреждённый кабель. Недостатком этой архитектуры является более высокая стоимость, более сложная структура.

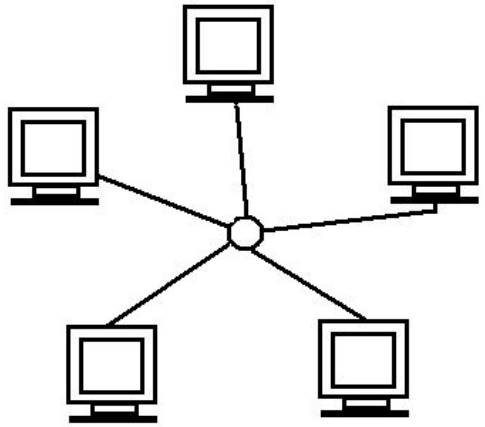

Рис.2. Структура звездообразной топологии вычислительной сети

1. Локальные компьютерные сети

Кольцевая типология. Сети рабочей станции связаны одна с другой по кругу. Сообщения такой сети циркулируют регулярно по кругу. Основная проблема, которая возникает в сетях кольцевой типологии, заключается в том, что каждая рабочая станция должна активно участвовать в пересылке информации, и в случае выхода из строя хотя бы одной из них вся сеть парализуется.

Данные передаются по кольцу от одного компьютера к другому, как правило, в одном направлении. Если компьютер распознает данные как «свои», то он копирует их себе во внутренний буфер. В сети с кольцевой топологией необходимо принимать специальные меры, чтобы в случае выхода из строя или отключения какой-либо станции не прервался канал связи между остальными станциями. Кольцо представляет собой очень удобную конфигурацию для организации обратной связи - данные, сделав полный оборот, возвращаются к узлу-источнику. Поэтому этот узел может контролировать процесс доставки данных адресату. Часто это свойство кольца используется для тестирования связности сети и поиска узла, работающего некорректно. Для этого в сеть посылаются специальные тестовые сообщения.

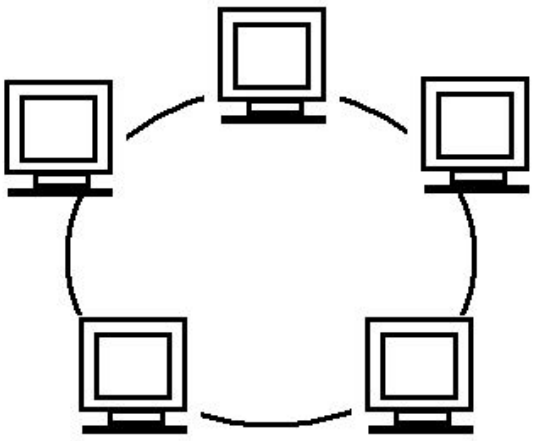

Рис.3. Структура кольцевой топологии вычислительной сети

1. Локальные компьютерные сети

Протоколы

На самом низком уровне компьютеры обмениваются пакетами сообщений, которые включают адрес отправителя, адрес получателя, характеристики, определяющие содержимое пакета, собственно данные, а также специализированные данные (контрольную сумму пакета, CRC), используемые для обнаружения ошибок передачи.

Пакеты могут вкладываться друг в друга. На вложении пакетов сообщений основано понятие протоколов.

Протокол - это стандарт, определяющий структуру и порядок интерпретации передаваемых пакетов данных.

При передаче данных в сети одновременно может использоваться несколько протоколов, которые наслаиваются один на другой. Протокол верхнего уровня вкладывается в протокол более низкого уровня и т.д.

В сильно упрощенном виде процесс передачи данных в сети реализуется следующим образом.

Протокол верхнего уровня определяет запрос на получение данных или содержит сами данные. В этом протоколе нет никаких сведений о способах передачи данных и типе передающего адаптера. Сформированный таким образом пакет данных передается программе, обслуживающей передачу данных в сети, которая “вкладывает” его в протокол транспортного уровня, "приписывая" заголовок и окончание, соответствующие этому протоколу. Далее, полученный пакет передается протоколу нижнего уровня, соответствующего используемому сетевому адаптеру. Его программно-аппаратное обеспечение присоединяет к пакету заголовок и окончание соответствующего протокола.

Далее, пакет передается по сетевому кабелю, где его принимает адаптер компьютера-адресата. Средствами сетевого адаптера убираются заголовок и окончание протокола нижнего уровня. Далее, пакет передается программе, обслуживающей передачу данных (транспортный уровень). Она проверяет правильность передачи, убирает “свои” заголовок и окончание и передает пакет программе, обслуживающей протокол верхнего уровня. Он выделяет из пакета данные и передает их программе, которой они предназначены.

За счет вложенности протоколов реализуется независимость программного обеспечения, реализующего обработку данных, от особенностей их передачи, а также программ, обслуживающих передачу данных от используемых сетевых адаптеров.

Самая общая модель обмена данными в сети OSI (Open System Itnterconnection) предполагает наличие 7 уровней протоколов. Однако в большинстве случаев все 7 уровней не используются.

- Протоколы нижнего уровня соответствуют типам сетевых адаптеров (Ethernet, Token Ring, FDDI).
- Протоколы среднего (транспортного) уровня обеспечивают компоновку и контроль передачи пакетов сообщений (NetBIOS, SPX/IPX, TCP/IP).
- Протоколы верхнего уровня обеспечивают обращение к файлам других компьютеров. Когда программа запрашивает обращение к данным того или иного файла, программа обслуживания файловой системы ОС проверяет, находится ли он на дисках данного компьютера. Если это так, то обращение к этому файлу производится стандартным для данной ОС и данной файловой системы способом. Если обнаруживается, что файл размещен на другом компьютере и доступ к нему с данного компьютера данному пользователю разрешен, то вступает в действие рассмотренный выше механизм передачи пакетов сообщений.

1. Локальные компьютерные сети

Организация передачи данных в сети

Необходимым условием работы единой локальной сети является использование сетевой операционной системы. Такие операционные системы обеспечивают совместное использование не только аппаратных ресурсов сети (принтеров, накопителей и т. д.), но и распределенных коллективных технологий при выполнении разнообразных работ. Наибольшее распространение получили сетевые операционные системы Novell NetWare, Linux и Windows.

Информация в сетях передается отдельными порциями — пакетами, причем длина этих пакетов строго ограничена (обычно величиной в несколько килобайтов). Этот способ передачи связан с тем, что локальная сеть должна обеспечивать качественную связь для всех компьютеров сети за разумное время доступа — время ожидания пользователем начала связи.

Компьютерные сети породили новые технологии обработки информации – сетевые технологии, позволяющие совместно использовать аппаратные и программные средства. Для сотрудников многих учреждений стало привычным пользоваться электронной почтой для обмена сообщениями и документами, для совместной работы. На предприятиях на базе локальных сетей создаются автоматизированные системы управления предприятием и технологическими процессами.

Распространенный способ организации обработки информации в сети называется технологией «клиент—сервер». В ней предполагается глубокое разделение функций компьютеров в сети.

Основная функция сервера — выполнение специфических действий по запросам клиента (например, решение сложной математической задачи, поиск данных в базе данных, соединение клиента с другим клиентом ит. д.).

Способы организации многопользовательской работы

Программное обеспечение, предназначенное для использования в компьютерных сетях, разделяется на серверное и клиентское ПО, а также ПО промежуточного уровня (middleware).

Важнейшей частью системного серверного ПО являются сетевые ОС, управляющие работой сетей с выделенным сервером. Для небольших и средних сетей - это Novell NetWare, Windows NT/2000/2003 Server, различные версии ОС Unix. При необходимости создания одноранговой сети можно использовать Windows 95/98/ME/NT Workstation/2000/XP.

Специализированное серверное ПО используется для выполнения специфических функций обслуживания пользователей сети. Это, например, SQL-серверы обслуживающие работу с единой базой данных, которые могут одновременно взаимодействовать с несколькими прикладными программами, выполняющимися на рабочих станциях.

В качестве клиентского системного ПО может выступать практически любая ОС.

ПО промежуточного уровня предназначено для повышения эффективности доступа к серверному ПО.

1. Локальные компьютерные сети

Прикладное программное обеспечение, предназначенное для работы в сети, часто разделяется на клиентскую и серверную части.

Коллективная работа группы пользователей возможна на основе централизованной или распределенной обработки данных.

Централизованная обработка данных - это способ организации работы, при котором все функции обработки данных, необходимые различным пользователям, выполняются одной или несколькими ЭВМ коллективного использования. В этом случае все данные хранятся на ЭВМ коллективного использования и полностью обрабатываются на ней. К такой ЭВМ пользователи подключаются через терминалы.

Терминал - это устройство, обеспечивающее передачу и прием данных от ЭВМ.

Терминал не может обрабатывать данные, но имеет клавиатуру, дисплей и блок связи с ЭВМ.

Распределенная обработка данных - это способ организации работы, при котором данные и функции их обработки распределены между несколькими индивидуально и коллективно используемыми ЭВМ.

Распределенная обработка данных возможна как при автономном функционировании ЭВМ отдельных рабочих мест, так и при их объединении в вычислительную сеть.

Сетевые системы обработки данных могут быть построены на основе архитектур файл-сервер и клиент-сервер.

При построении системы обработки данных в архитектуре файл-сервер общие для нескольких пользователей данные хранятся на сетевом сервере, но их обработка выполняется на ЭВМ рабочего места. Программа, выполняющаяся на рабочей станции, запрашивает данные нужного ей файла у функционирующей на сервере сетевой ОС. Сервер считывает искомые данные из указанного файла и передает их рабочей станции. На ней эти данные обрабатываются, а результаты обработки могут быть опять переданы серверной ОС, для размещения их в файлах сетевого сервера.

Достоинством архитектуры файл-сервер является то, что прикладная программа включает только клиентскую часть, а обращение к файлам, размещенным на сервере, производится общесистемными средствами обслуживания сети. Однако в этом случае, при необходимости отобрать только определенный фрагмент данных того или иного файла, последний полностью пересылается по каналам сети на рабочую станцию. Если в сети одновременно работает много пользователей, и они интенсивно обращаются к данным, хранящимся на сервере, сеть сильно перегружается и выполнение прикладных программ может очень замедлиться из-за ожидания окончания процедур пересылки данных.

При построении систем в архитектуре "клиент-сервер" часть функций обработки данных выполняется сервером, а часть - клиентом. Если прикладной программе, выполняющейся на рабочей станции, нужны данные, удовлетворяющие определенным критериям, то она только выдает запрос серверной части программы на их выборку. Серверная компонента программы отбирает данные по этому запросу и пересылает по сети только их. Например, прикладная программа передает запрос на выборку данных SQL-серверу. Тот обрабатывает запрос к базе данных и передает по сети на рабочую станцию только необходимые данные. За счет этого становится возможным существенно уменьшить объем пересылаемых по сети данных. Специально отметим, что при использовании архитектуры файл-сервер такой отбор не производится и по сети пересылается вся база данных и отбор выполняется рабочей станции.

При использовании архитектуры клиент-сервер, помимо доступа к данным серверная часть программы может выполнять еще и определенные действия по их обработке. Более того, в ряде случаев реализуется даже эмуляция централизованной обработки данных, когда все функции их обработки выполняются сервером. В этом случае с рабочей станции на сервер передаются только сведения о нажатых пользователем клавишах и перемещениях мыши, а с сервера на нее поступают только образы представления данных на экране монитора, которые также формируются сервером. То есть, фактически, ПК на время превращается в терминал.

Построение систем обработки данных в архитектуре клиент-сервер возможно на основе моделей "толстого" и "тонкого" клиентов. В модели "толстого" клиента сервер выполняет только функции отбора данных, а их прикладная обработка выполняется на рабочей станции. В модели "тонкого" клиента сервер выполняет отбор данных и их обработку, а на рабочую станцию пересылаются только результаты обработки.

Различают также двух-, трех- и многоуровневую архитектуру клиент-сервер. При двухуровневой архитектуре система обработки данных включает клиентскую и единую серверную компоненты. При трехуровневой архитектуре серверная компонента делится на сервер базы данных и сервер приложений. В качестве сервера базы данных обычно выступает SQL-сервер. Сервер приложений выступает в роли промежуточного уровня ПО сетевой системы обработки данных (middleware). Обычно в его функции входит реализация наиболее сложных и общих процедур прикладной обработки данных, требующих постоянного взаимодействия с большими информационными массивами, управляемыми сервером базы данных.

1. Локальные компьютерные сети

Сервер базы данных и сервер приложений могут выполняться на одной или на разных ЭВМ. Трехуровневая архитектура обычно соответствует модели тонкого клиента, а двухуровневая - модели толстого клиента. Но модель тонкого клиента можно организовать и при двухуровневой архитектуре. В этом случае единая серверная компонента совмещает функции доступа к данным и их обработки.

В общем случае, функции большинства систем обработки данных можно разделить на четыре группы:

а) функции представления данных;

б) функции обработки данных;

в) функции доступа к структурированной информации;

г) функции доступа к файлам.

Функции представления данных - это операции организации взаимодействия программы с пользователем, связанные с отображением данных на экране монитора и при печати, приема данных, вводимых с помощью устройств ввода информации в ЭВМ и т.д.

Функции обработки данных - это операции, связанные с непосредственной реализацией алгоритмов обработки исходных данных и получением результатной информации.

Функции доступа к структурированной информации - это операции интерпретации и извлечения данных из информационных массивов, в которых они хранятся, и записи их в эти массивы с учетом заданной логической и физической структуры их размещения на носителях данных.

Функции доступа к файлам - это операции непосредственного доступа к файлам, в которых хранятся используемые программой информационные массивы. Обычно реализуются средствами ОС.

Распределение функций обработки данных при различных способах организации многопользовательской работы представлено в следующей таблице.

При централизованной обработке данных рабочие места оснащаются терминалами, а все остальные операции выполняются одной или несколькими центральными ЭВМ. Терминалы исполняют только функции отображения и ввода данных. Функции представления данных распределены между ними и центральной ЭВМ, поскольку именно последняя формирует образы экранов, отображаемых терминалами. То есть выполняет еще и часть функций представления данных.

При автономном функционировании рабочих мест все функции исполняются установленными на них ПК.

В системах сетевой обработки данных, основанных на архитектуре файл-сервер, в функции сетевого сервера входит только реализация операций доступа к файлам, а функции представления данных, их обработки и доступа к структурированной информации реализуются программным обеспечением, исполняющимся на ПК отдельных рабочих мест.

В системах, построенных в архитектуре клиент-сервер на основе модели толстого клиента, серверные компоненты выполняют функции доступа к массивам структурированной информации и хранящим их файлам. Функции представления данных и их обработки полностью реализуются программным обеспечением, выполняющимся на рабочих станциях.

При построении системы на основе модели архитектуры тонкого клиента, функции доступа к массивам структурированной информации и хранящим их файлам полностью выполняются серверным программным обеспечением, а функции обработки данных могут быть разделены между клиентской и серверной компонентами. Функции представления данных полностью выполняются клиентской компонентой.

При реализации архитектуры клиент-сервер в режиме эмуляции централизованной обработки на рабочих станциях выполняются только функции представления данных. При этом часть этих функций перенесена на сервер, поскольку именно он формирует образы экранов и пересылает их клиентской стороне, которая занята только их отображением. Отличие полностью централизованной обработки от режима ее эмуляции состоит в том, что в первом случае рабочее место оборудовано терминалом, который в состоянии только отображать и вводить данные, но не может их обрабатывать, а во втором - персональным или сетевым компьютером, который может исполнять программы. Если на рабочем месте установлен полноценный ПК, то он может для одного приложения работать в режиме эмуляции централизованной обработки, то есть выполнять только функции терминала, а другие приложения исполнять самостоятельно. Например, какая-то программа может полностью исполняться на сервере, а ПК будет только отображать полученные результаты и вводить данные, но наряду с этим на нем же параллельно может быть запущен текстовый процессор, все функции которого будут полностью выполняться с использование аппаратных ресурсов данного ПК.

2. Защита информации. Антивирусная защита сети

Защита информации

В наше время большая часть информации хранится в цифровом виде. Проблема защиты информации принимает глобальный характер. Государством принимаются специальные законы о защите информации.

Цифровая информация – информация, хранение, передача и обработка которой осуществляется средствами ИКТ.

Можно различить два основных вида угроз для цифровой информации:

- кража или утечка информации;
- разрушение, уничтожение информации.

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

Утечка информации представляет собой кражу или копирование информации. Если компьютер подключен к глобальной сети, то он потенциально доступен для проникновения в его информационную базу извне.

Разрушение информации может быть несанкционированным и непреднамеренным.

Непреднамеренное воздействие – происходит вследствие ошибок пользователя, из-за сбоев в работе оборудования или программного обеспечения. Могут возникнуть непредвиденные внешние факторы: авария электросети, пожар или землетрясение.

Несанкционированное воздействие – это преднамеренная порча или уничтожение информации.

К несанкционированному вмешательству относится криминальная деятельность хакеров – «хакеров» информационных систем с целью воздействия на их содержание и работоспособность. Например, для снятия денег с чужого счета в банк, для уничтожения данных следственных органов и т.п. Большой вред корпоративным информационным системам наносят так называемые хакерские атаки – одновременное обращение с большого количества компьютеров на сервер информационной системы. Сервер не справляется с количеством запросов, что приводит к «зависанию» в его работе.

К этой категории угроз относится деятельность людей, занимающихся созданием и распространением компьютерных вирусов.

Компьютерные вирусы

Компьютерные вирусы – вредоносные программные коды, способные нанести ущерб данным на компьютере или вывести его из строя.

Компьютерные вирусы являются программами, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

Первая массовая эпидемия компьютерного вируса произошла в 1986 году, когда вирус Brain «заражал» дискеты для первых массовых персональных компьютеров. В настоящее время известно несколько десятков тысяч вирусов, заражающих компьютеры с различными операционными системами и распространяющихся по компьютерным сетям.

Обязательным свойством компьютерного вируса является способность к размножению (самокопированию) и незаметному для пользователя внедрению в файлы, загрузочные секторы дисков и документы. Название «вирус» по отношению к компьютерным программам пришло из биологии именно по признаку способности к саморазмножению.

Так же, как и биологические вирусы, компьютерные вирусы имеют три функции: размножение, рост и заражение.

После заражения компьютера вирус может активизироваться и заставить компьютер выполнять какие-либо действия. Активизация вируса может быть связана с различными событиями (наступлением определенной даты или дня недели, запуском программы, открытием документа и так далее).

Кроме вирусов-разрушителей существуют вирусы-шпионы. Их называют троянцами. Внедрившись в операционную систему, троянец может тайно пересылать заинтересованным лицам конфиденциальную информацию.

2. Защита информации. Антивирусная защита сети

Меры защиты информации

Принимаемые для защиты информации меры в первую очередь зависят от уровня его использования, от значимости информации и степени ущерба, который может нанести владельцу ее утечка или разрушение.

Если один и тот же компьютер используется многими лицами и личная информация каждого требует защиты от доступа посторонних, то с помощью системных средств организуется разграничение доступа для разных пользователей. Для этого создаются учетные записи пользователей, устанавливаются пароли.

Для защиты компьютеров, подключенных к глобальной сети от подозрительных объектов используются защитные программы – брандмауэры. Например, пользователь может запретить прием посланий по электронной почте с определенных адресов или определенного содержания. Брандмауэры могут предотвращать атаки, фильтровать ненужные рекламные рассылки.

Главной опасностью является потеря данных по непреднамеренным причинам, а также из-за проникновения вирусов.

Основные правила безопасности:

- периодически осуществлять резервное копирование (файлы с наиболее важными данными дублировать и сохранять на внешних носителях);
- использовать блок бесперебойного питания (чтобы избежать потери информации из-за внезапного отключения электроэнергии или скачков напряжения в сети);
- регулярно осуществлять антивирусную проверку компьютера.

Антивирусные программы

Основным разносчиком вирусов является нелицензионное программное обеспечение, файлы, скопированные из случайных источников а также службы Интернета: электронная почта, Всемирная паутина – WWW. Каждый день в мире появляются сотни новых компьютерных вирусов. Борьбой с вирусами занимаются специалисты, создающие антивирусные программы.

Лицензионные антивирусные программы следует покупать у фирм-производителей. Антивирусную программу недостаточно лишь однажды установить на компьютер. Необходимо регулярно обновлять ее базу – добавлять настройки на новые типы вирусов. Наиболее оперативно такое обновление производится через Интернет серверами фирм-производителей. Антивирусные программы могут использовать различные принципы для поиска и лечения зараженных файлов.

Полифаги

Самыми популярными и эффективными антивирусными программами являются антивирусные программы полифаги (например, Kaspersky Anti-Virus, Dr.Web). Принцип работы полифагов основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых (неизвестных полифагу) вирусов.

Для поиска известных вирусов используются так называемые маски. Маской вируса является некоторая постоянная последовательность программного кода, специфичная для этого конкретного вируса. Если антивирусная программа обнаруживает такую последовательность в каком-либо файле, то файл считается зараженным вирусом и подлежит лечению.

Для поиска новых вирусов используются алгоритмы «эвристического сканирования», то есть анализ последовательности команд в проверяемом объекте. Если «подозрительная» последовательность команд обнаруживается, то полифаг выдает сообщение о возможном заражении объекта.

Полифаги могут обеспечивать проверку файлов в процессе их загрузки в оперативную память. Такие программы называются антивирусными мониторами.

К достоинствам полифагов относится их универсальность. К недостаткам можно отнести большие размеры используемых ими антивирусных баз данных, что приводит к относительно небольшой скорости поиска вирусов.

2. Защита информации. Антивирусная защита сети

Ревизоры

Принцип работы ревизоров (например, Adinf) основан на подсчете контрольных сумм для присутствующих на диске файлов. Эти контрольные суммы затем сохраняются в базе данных антивируса, как и некоторая другая информация: длины файлов, даты их последней модификации и пр.

При последующем запуске ревизоры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то ревизоры сигнализируют о том, что файл был изменен или заражен вирусом.

Недостаток ревизоров состоит в том, что они не могут обнаружить вирус в новых файлах (на дискетах, при распаковке файлов из архива, в электронной почте), поскольку в их базах данных отсутствует информация об этих файлах.

Блокировщики

Антивирусные блокировщики — это программы, перехватывающие «вирусоопасные» ситуации и сообщающие об этом пользователю. К таким ситуациям относится, например, запись в загрузочный сектор диска. Эта запись происходит при установке на компьютер новой операционной системы или при заражении загрузочным вирусом.

Наибольшее распространение получили антивирусные блокировщики в BIOS компьютера. С помощью программы BIOS Setup можно провести настройку BIOS таким образом, что будет запрещена (заблокирована) любая запись в загрузочный сектор диска и компьютер будет защищен от заражения загрузочными вирусами. К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения.