**Практическая работа № 14** Разграничение прав доступа в сети, общее дисковое пространство в локальной сети. Защита информации, антивирусная защита.

**Цель:**освоение приемов обмена файлами между пользователями локальной компьютерной сети; осуществление защиты информации.

***Краткие теоретические сведения***

**1. Виды компьютерных сетей.**

Одним из самых значительных достижений прошлого века считается развитие информационных технологий — компьютерных технологий хранения, преобразования и передачи информации. Важнейшую роль в информационном скачке человечества сыграло создание коммуникационных компьютерных сетей.

Совокупность компьютеров, взаимосвязанных между собой каналами передачи информации и распределенных по некоторой территории, называется компьютерной сетью. Существующие в настоящий момент многочисленные компьютерные *сети принято делить по так называемому территориальному признаку:*

* GAN (Global Area Network – глобальная сеть), общее планетное соединение компьютерных сетей - Интернет;
* WAN (Wide Area Network – широкомасштабная сеть), континентальное на уровне государства объединение компьютерных сетей;
* MAN (Metropolitan Area Network – междугородняя сеть), междугороднее и областное объединение компьютерных сетей;
* LAN (Local Area Network – локальная сеть) сетевое соединение, функционирующее обычно в стенах одной организации.

WAN и MAN – региональные сети. Деление на WAN и MAN компьютерные сети в настоящее время является весьма условным, поскольку сейчас каждая региональная сеть представляет собой, как правило, часть какой-нибудь глобальной сети.

Многие организации, заинтересованные в защите информации от несанкционированного доступа (например, военные, банковские и пр.), создают собственные, так называемые корпоративные сети. Корпоративная сеть может объединять тысячи и десятки тысяч компьютеров, размещенных в различных странах и городах (в качестве примера можно привести сеть корпорации Microsoft, MSN).

## 2. Локальная компьютерная сеть.

Важной отличительной особенностью любой локальной сети является то, что для соединения компьютеров в такой сети не нужно использовать телефонную сеть — компьютеры расположены достаточно близко друг от друга и соединяются кабелем.

Посредством ЛС в систему объединяются персональные компьютеры, расположенные на многих удаленных рабочих станциях, которые используют совместно оборудование, программные средства и информацию. Рабочие места сотрудников перестают быть изолированными и объединяются в единую систему.

Рассмотрим *преимущества, получаемые при сетевом объединении персональных компьютеров в виде внутрипроизводственной вычислительной сети.*

1. Разделение ресурсов: разделение ресурсов позволяет экономно использовать ресурсы, например, управлять периферийными устройствами, такие как лазерное печатающее устройство, со всех присоединенных рабочих станций.
2. Разделение данных: разделение данных предоставляет возможность доступа и управления базами данных с периферийных рабочих мест, нуждающихся в информации.
3. Разделение программных средств: разделение программных средств, предоставляет возможность одновременного использования централизованных, ранее установленных программных средств.
4. Разделение ресурсов процессора: при разделение ресурсов процессора возможно использование компьютерных мощностей для обработки данных другими системами , входящими в сеть. Предоставляемая возможность заключается в том, что на имеющиеся ресурсы не "набрасываются" моментально, а только лишь через специальный процессор, доступный каждой рабочей станции.
5. Многопользовательский режим: многопользовательские свойства системы содействуют одновременному использованию централизованных прикладных программных средств, ранее установленных и управляемых, например, если пользователь системы работает с другими заданиями, то текущая выполняемая работа отодвигается на задний план.
6. Электронная почта: с помощью электронной почты происходит интерактивный обмен информацией между рабочей станцией и другими станциями, установленными в вычислительной сети.

**3. Компоненты локальной сети.**

Локальная сеть, как правило, состоит из следующих компонентов.

1. Файл-сервер - центральная машина, имеющая большую дисковую память.
2. Рабочие станции - множество компьютеров, подключенных к центральной машине (файловому серверу).
3. Сетевые платы. В каждый компьютер, который мы собираемся подключить к локальной сети, следует установить дополнительную сетевую плату— контроллер. Ее назначение, как и любого другого контроллера, заключается в преобразовании сигналов, идущих из сети, в сигналы, поступающие на блоки компьютера, а также в выполнении обратной операции. Сетевая плата вставляется в свободный слот на материнской плате, а к ее гнезду, находящемуся на задней стенке системного блока, подключается коаксиальный кабель. Серверу необходима сетевая плата повышенной производительности, т.е. ее производительность должна быть больше производительности сетевых плат для локальных рабочих мест.
4. Соединительный кабель. Кабель соединяет друг с другом сетевые платы рабочих мест (компьютеров). Кабельные системы - основа коммуникаций. При выборе типа кабеля учитываются следующие показатели:

* стоимость монтажа и обслуживания,
* скорость передачи информации,
* ограничения на величину расстояния передачи информации,
* безопасность передачи информации.

**Периферийное оборудование.** К файловому серверу подключается периферийное оборудование (например, лазерное устройство печати, графопостроитель и другие).

**Операционная система вычислительной сети.**Как и любая вычислительная система нуждается в операционной системе, так и ЛС нуждается в собственной операционной системе. На файл-сервере необходимо установить специальную программу-драйвер для управления сетью. При загрузке сети драйвер сети должен включаться первым. Драйвер сети следует установить и на всех остальных компьютерах сети, но на сервере он устанавливается в полной форме, там же задаются все параметры сети.

Прикладное программное обеспечение должно быть разработано специально для компьютерных сетей. Необходимо предусмотреть возможность управления доступом к имеющимся ресурсам системы со всех подключенных рабочих мест.

## 4. Топология локальных сетей

4.1 Топология типа звезда.

Концепция топологии сети в виде звезды пришла из области больших ЭВМ, в которой головная машина получает и обрабатывает все данные с периферийных устройств как активный узел обработки данных. Вся информация между двумя периферийными рабочими местами проходит через центральный узел вычислительной сети (сервер). Роль центрального узла может выполнять специализированное устройство - концентратор (hub - англ.)

Пропускная способность сети определяется вычислительной мощностью узла и гарантируется для каждой рабочей станции. Коллизий (столкновений) данных не возникает.

Кабельное соединение довольно простое, так как каждая рабочая станция связана с узлом. Затраты на прокладку кабелей высокие, особенно когда центральный узел географически расположен не в центре топологии.

При расширении вычислительных сетей не могут быть использованы ранее выполненные кабельные связи: к новому рабочему месту необходимо прокладывать отдельный кабель из центра сети.

Топология в виде звезды является наиболее быстродействующей из всех топологий вычислительных сетей, поскольку передача данных между рабочими станциями проходит через центральный узел (при его хорошей производительности) по отдельным линиям, используемым только этими рабочими станциями. Частота запросов передачи информации от одной станции к другой невысокая по сравнению с достигаемой в других топологиях.

Производительность вычислительной сети в первую очередь зависит от мощности центрального концентратора. Он может быть узким местом вычислительной сети. В случае выхода из строя центрального узла нарушается работа всей сети.

*4.2 Кольцевая топология.*

При кольцевой топологии сети рабочие станции связаны одна с другой по кругу, т.е. рабочая станция 1 с рабочей станцией 2, рабочая станция 3 с рабочей станцией 4 и т.д. Последняя рабочая станция связана с первой. Коммуникационная связь замыкается в кольцо (рис. 14.2) .

Прокладка кабелей от одной рабочей станции до другой может быть довольно сложной и дорогостоящей, особенно если географически рабочие станции расположены далеко от кольца (например, в линию).

Основная проблема при кольцевой топологии 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. Неисправности в кабельных соединениях локализуются легко.

4.3 Шинная топология.

При шинной топологии среда передачи информации представляется в форме коммуникационного пути, доступного дня всех рабочих станций, к которому они все должны быть подключены. Все рабочие станции могут непосредственно вступать в контакт с любой рабочей станцией, имеющейся в сети.

Рабочие станции в любое время, без прерывания работы всей вычислительной сети, могут быть подключены к ней или отключены. Функционирование вычислительной сети не зависит от состояния отдельной рабочей станции.

**5. Обмен файлами между пользователями локальной компьютерной сети.**Чтобы переслать файл на другой компьютер сети, необходимо открыть папку Мой компьютер ◊ссылка Сетевое окружение. Если компьютеры локальной сети не высвечиваются, выбрать ссылку Отобразить компьютеры рабочей группы. Затем открыть папку нужного компьютера и стандартным образом производить операции чтения/копирования файлов с одного ПК на другой.

**6. Вредоносная программа**— компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе, либо для скрытого нецелевого использования ресурсов системы, либо иного воздействия, препятствующего нормальному функционированию компьютерной системы. К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

Независимо от типа, вредоносные программы способны наносить значительный ущерб, реализуя любые угрозы информации — угрозы нарушения целостности, конфиденциальности, доступности.

**6.1. Сетевые черви.** К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

* проникновения на удаленные компьютеры;
* запуска своей копии на удаленном компьютере;
* дальнейшего распространения на другие компьютеры в сети.

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д.

Некоторые черви обладают свойствами других разновидностей вредоносного программного обеспечения. Например, некоторые черви содержат троянские функции или способны заражать выполняемые файлы на локальном диске, т. е. имеют свойство троянской программы и/или компьютерного вируса.

**6.2. Классические компьютерные вирусы.** К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью:

* последующего запуска своего кода при каких-либо действиях пользователя;
* дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

* при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
* вирус скопировал себя на съёмный носитель или заразил файлы на нем;
* пользователь отослал электронное письмо с зараженным вложением.

**6.3. Троянские программы.** В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для массированных DoS-атак на удалённые ресурсы сети).

**6.4. Хакерские утилиты** и прочие вредоносные программы. К данной категории относятся:

* утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
* программные библиотеки, разработанные для создания вредоносного ПО;
* хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
* «злые шутки», затрудняющие работу с компьютером;
* программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
* прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.

*Руткит (Rootkit)*- программа или набор программ, использующих технологии сокрытия системных объектов (файлов, процессов, драйверов, сервисов, ключей реестра, открытых портов, соединений и пр.) посредством обхода механизмов системы.

В системе Windows под термином руткит принято считать программу, которая внедряется в систему и перехватывает системные функции, или производит замену системных библиотек. Кроме того, многие руткиты могут маскировать присутствие в системе любых описанных в его конфигурации процессов, папок и файлов на диске, ключей в реестре. Многие руткиты устанавливают в систему свои драйверы и сервисы (они естественно также являются «невидимыми»).

В последнее время угроза руткитов становится все более актуальной, т.к. разработчики вирусов, троянских программ и шпионского программного обеспечения начинают встраивать руткит-технологии в свои вредоносные программы. Одним из классических примеров может служить троянская программа Trojan-Spy.Win32.Qukart, которая маскирует свое присутствие в системе при помощи руткит-технологии. Ее RootKit-механизм прекрасно работает в Windows 95, 98, ME, 2000 и XP.

*Современные антивирусные программы*обеспечивают комплексную защиту программ и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер (Интернет, локальная сеть, электронная почта, съемные носители информации). Большинство антивирусных программ сочетает в себе функции постоянной защиты (антивирусный монитор) и функции защиты по требованию пользователя (антивирусный сканер).

*Межсетевой экран*— это программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа к компьютеру. Другое распространенное название сетевого экрана — файервол от английского термина firewall. Иногда сетевой экран называют еще брандмауэром (нем. brandmauer) — это немецкий эквивалент слова firewall. Основная задача сетевого экрана — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации сетевого экрана. Межсетевой экран позволяет:

* Блокировать хакерские атаки;
* Не допускать проникновение сетевых червей;
* Препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.

***Практические задания***

**Задание №1**. Составьте схему локальной сети компьютерного класса в программе MS Word

**Задание №2**

1. Создайте на  сетевом диске папку под именем*Почта\_1*(цифра в имени соответствует номеру вашего компьютера).
2. С помощью текстового редактора Word создайте письмо к одногруппникам(текст - ответ на вопрос, номер вопроса - номер вашего ПК). Письмо должно начинаться с ваших данных: ФИО, № вашего ПК.
3. Сохраните данный текст в папке *Почта\_1*своего компьютера в файле *письмо Х.doc*, где *Х*– номер компьютера.
4. Откройте папку другого компьютера, например, *Почта\_2*и скопируйте в него файл*письмо1*из своей папки*Почта\_1*.
5. Попробуйте отправить письмо на компьютер преподавателя.
6. В своей папке *Почта\_1*прочитайте письма от других пользователей, например*письмо2*. Допишите в них свой ответ.
7. Переименуйте файл *письмо2 .doc* в файл *письмо2\_ответ1.doc*
8. Переместите файл *письмо2\_ответ1.doc* в папку *Почта \_2*и удалите его из своей папки
9. Далее повторите п.2-4 для других компьютеров.
10. Прочитайте сообщения от других пользователей в своей папке и повторите для них действия п.5-8.
11. Запишите в отчет по практической работе, на какие рабочие станции вы скопировали свой файл, и с каких рабочих станций скопировали файлы.

***Контрольные вопросы***

1.Укажите основное назначение компьютерной сети.

2. Укажите объект, который является абонентом сети.

3. Укажите основную характеристику каналов связи.

4. Что такое локальная сеть, глобальная сеть?

5. Что понимается под топологией локальной сети?

6. Какие существуют виды топологии локальной сети?

7. Охарактеризуйте кратко каждую топологию.

8. Как классифицируют сети по территориальному признаку?

9. Как посмотреть информацию, находящуюся на другой рабочей станции?

10. Что понимают под вредоносными программами?

11. Какие программы называют троянскими?

12. Какие программы называют червями?

13. Как попадают на компьютер классические вирусы. Какой вред они наносят?

14. Какие существуют способы защиты от вредоносных программ?

15. Какие функции сочетают в себе современные антивирусные программы?

16. Что такое межсетевой экран?