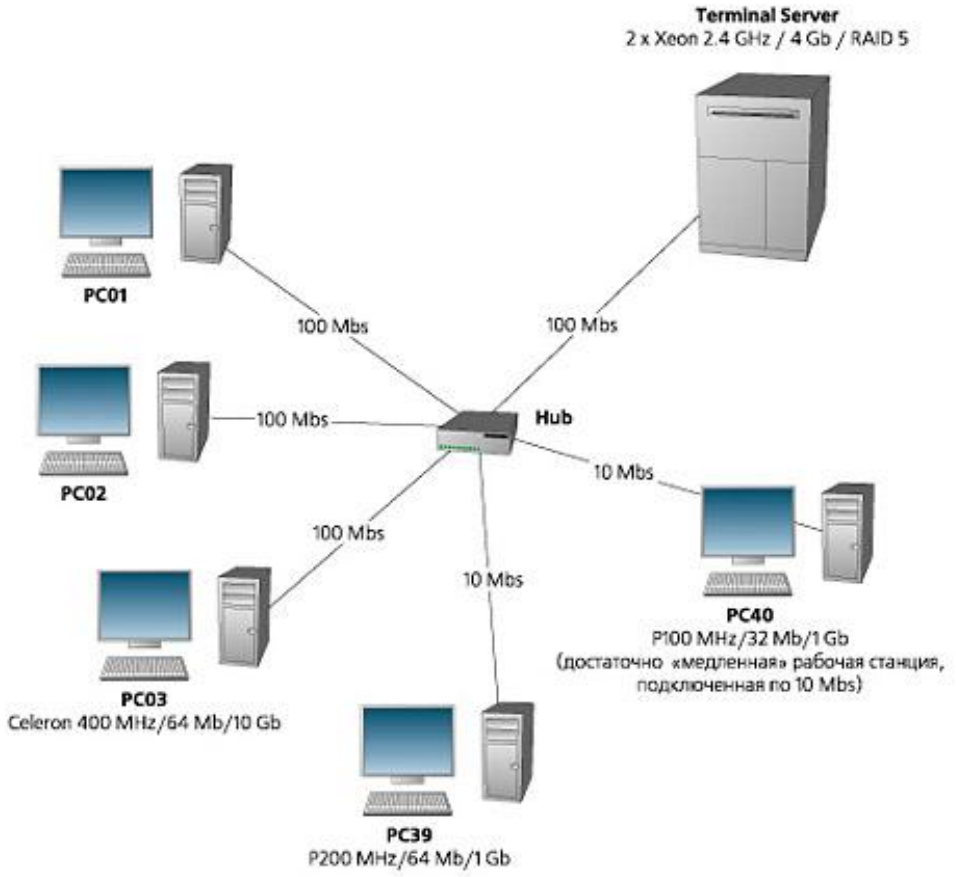
ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Проблема защиты информации от несанкционированного доступа особо обострилась с широким распространением локальных и, особенно, глобальных компьютерных сетей.



Защита информации в локальных сетях

Зачастую ущерб наносится из-за элементарных ошибок пользователей, которые случайно портят или удаляют жизненно важные данные.

Необходимо разграничение полномочий пользователей.

ПРИМЕР

Оснастить сервер или сетевые рабочие станции устройством чтения смарт-карточек и специальным программным обеспечением

- **Для доступа к компьютеру пользователь должен вставить смарт-карту в устройство чтения и ввести свой персональный код**
- **Программное обеспечение позволяет установить несколько уровней безопасности, которые управляются системным администратором**

Защита информации при удалённом доступе

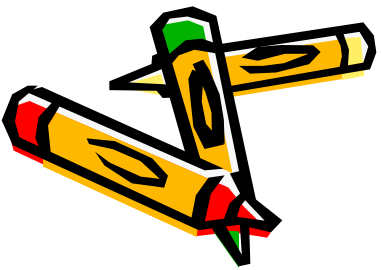
Чаще всего для организации удаленного доступа используются кабельные линии (обычные телефонные или выделенные) и радиоканалы.

В связи с этим защита информации, передаваемой по каналам удаленного доступа, требует особого подхода.

ПРИМЕР №1

В мостах и маршрутизаторах удаленного доступа применяется

- **сегментация пакетов – это их разделение и передача параллельно по двум линиям**
- **процедура сжатия передаваемых пакетов - гарантия невозможности расшифровки "перехваченных" данных**
- **ограничены в доступе к отдельным ресурсам сети главного офиса за счёт составления специальных программ**



ПРИМЕР №2

Специальные устройства контроля доступа к компьютерным сетям по коммутируемым линиям

модуль Remote Port Security Device (PRSD) позволяет установить несколько уровней защиты и контроля доступа:

- **шифрование данных, передаваемых по линии при помощи генерируемых цифровых ключей;**
- **контроль доступа в зависимости от дня недели или времени суток (всего 14 ограничений).**

КОМПЬЮТЕРНЫЕ ВИРУСЫ

АНТИВИРУСНЫЕ ПРОГРАММЫ

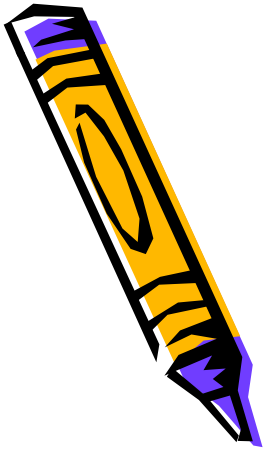
Компьютерный вирус

специально написанная небольшая программа, которая может приписывать себя к другим программам (то есть заражать их), а также выполнять различные вредные действия на компьютере

Признаки заражения компьютера

- некоторые программы перестают работать или работают с ошибками;
- размер некоторых исполнимых файлов и время их создания изменяются;
- на экран выводятся посторонние символы и сообщения, появляются странные видео и звуковые эффекты;
- работа компьютера замедляется и уменьшается размер свободной оперативной памяти;
- некоторые файлы и диски оказываются испорченными (иногда необратимо, если вирус отформатирует диск);
- компьютер перестает загружаться с жесткого диска.

Пути заражения компьютера вирусами



через зараженные дискеты

через компьютерную сеть

Самозародиться вирусы не могут - это программа, специально написанная человеком для разрушения программного обеспечения компьютера и его системных областей. Типичный размер вируса составляет от десятков байт до десятков килобайт.

Типы компьютерных вирусов

1 Файловые вирусы, поражающие exe и com файлы, иногда только com.

Заражение происходит при запуске зараженной программы (хотя бы однократном

Первым заражается командный процессор, а через него все остальные программы

Такие вирусы портят программы и данные, но иногда могут уничтожить содержимое всего жесткого диска.

Наиболее опасны резидентные вирусы, которые остаются в оперативной памяти постоянно

Типы компьютерных вирусов

2

**Загрузочные вирусы -
поражают загрузочные сектора жестких дисков и дискет**

Они наиболее опасны для компьютера, так как в результате их разрушительной работы компьютер перестает загружаться, иногда сразу после заражения, которое происходит даже при выводе оглавления зараженной дискеты.

Типы компьютерных вирусов

3

Вирусы, поражающие драйверы, указанные в файле config.sys, и дисковые файлы DOS.

Это ведет к прекращению загрузки компьютера.

Типы компьютерных вирусов

4

Вирусы DIR, меняющие файловую структуру.

Типы компьютерных вирусов

5

Невидимые вирусы или стелс-вирусы

Их очень трудно обнаружить. Простейший способ маскировки - при заражении файла вирус делает вид, что длина файла не изменилась.

Типы компьютерных вирусов

6

Самомодифицирующиеся вирусы

Они меняют свою структуру и код по случайному закону и их очень трудно обнаружить. Их называют также полиморфными. Две копии одного и того же вируса этого типа могут не содержать одинаковых последовательностей байт.

Типы компьютерных вирусов

7

Сетевые вирусы

Поражают машины, работающие в сети, в том числе в сети Интернет.

Типы компьютерных вирусов

8

Вирусы Word, Excel, Access, PowerPoint

Поражают документы и макросы программ из MS Office

Типы компьютерных вирусов

9

Вирусы Windows

Функционируют и портят данные в среде Windows

Методы борьбы с компьютерными вирусами

- ***Резервное копирование всех программ, файлов и системных областей дисков на дискеты, чтобы можно было восстановить данные в случае вируссной атаки. Создание системной и аварийной дискеты.***

Методы борьбы с компьютерными вирусами

- ***Ограничение доступа к машине путем введения пароля, администратора, закрытых дисков.***

Методы борьбы с компьютерными вирусами

- ***Включение антивирусного протектора от загрузочных вирусов в CMOS Setup машины. Защита дискет от записи.***

Методы борьбы с компьютерными вирусами

- ***Использование только лицензионного программного обеспечения, а не пиратских копий, в которых могут находиться вирусы.***

Методы борьбы с компьютерными вирусами

- ***Проверка всей поступающей извне информации на вирусы, как на дискетах, CD-ROM, так и по сети.***

Методы борьбы с компьютерными вирусами

- ***Применение антивирусных программ и обновление их версий.***

Методы борьбы с компьютерными вирусами

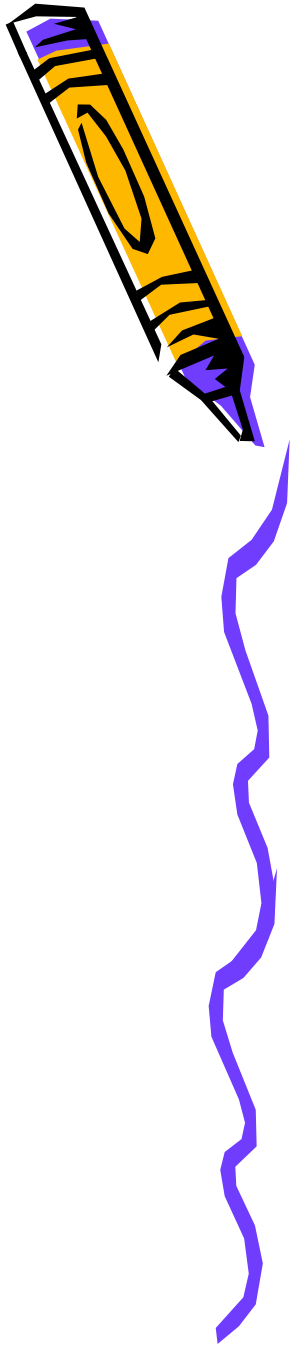
- ***Подготовка ремонтного набора дискет (антивирусы и программы по обслуживанию дисков).***

Методы борьбы с компьютерными вирусами

- ***Периодическая проверка компьютера на наличие вирусов при помощи антивирусных программ.***

Для защиты от вирусов и лечения зараженного компьютера используются антивирусные программы

Антивирусные программы



блокировщики

ревизоры

полифаги

Антивирусные блокировщики

резидентные программы, перехватывающие «вирусо-опасные» ситуации и сообщающие об этом пользователю

Например, «вирусо-опасной» является запись в загрузочные сектора дисков, которую можно запретить с помощью программы BIOS Setup.

Ревизоры

- Принцип работы ревизоров основан на подсчете контрольных сумм для хранящихся на диске файлов.
- Эти суммы, а также некоторая другая информация (длины файлов, даты их последней модификации и др.) сохраняются в базе данных антивируса.
- 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.

Полифаги

- Принцип работы полифагов основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных полифагу) вирусов.

- Для поиска известных вирусов используются маски вирусов (некоторая постоянная последовательность программного кода, специфичная для каждого конкретного вируса).

Наиболее эффективны

российские программы

Dr. Web, ADinf, AVP, BootCHK

зарубежные программы

Norton Antivirus, Dr. Solomon

Антивирусная база AVP для DOS и для Windows содержит информацию о более чем 28000 вирусов.

Правила

соблюдая которые можно предотвратить потерю ценной информации на случай сбоя или заражения машины вирусом

Правило N1. Создав любой новый файл (содержащий, например, текст, программу или рисунок), обязательно сразу скопируйте его на дискету.

Правило N2. Любую дискету, побывавшую на чужой машине, обязательно проверьте антивирусными программами с обновленными антивирусными базами.

Методы борьбы с компьютерными вирусами

- Резервное копирование всех программ, файлов
- Ограничение доступа к машине путем введения пароля
- Включение антивирусного протектора
- Защита дискет от записи.
- Использование только лицензионного программного обеспечения
- Проверка компьютера и всей поступающей извне информации на вирусы
- Применение антивирусных программ и обновление их версий