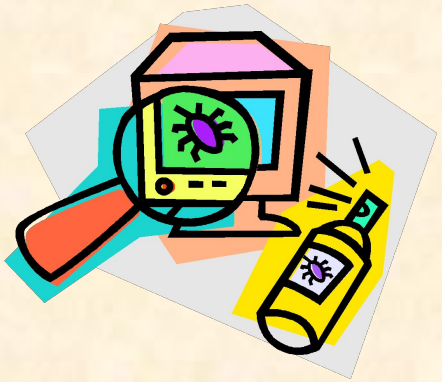
Сидоренко Анна Феликсовна
Трофимов Юрий Константинович

Вирусы и антивирусы



Термин

Вирус – компьютерная программа, способная к саморазмножению.

Существует масса других определений, можете попробовать дать свое…

Классификация

- Boot вирус
- Файловый вирус
- Макровирус
- Черви
- Почтовые вирусы

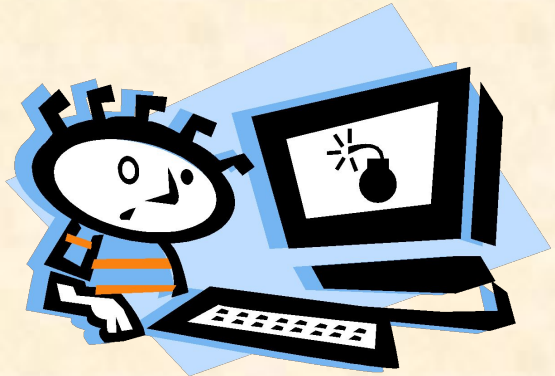
} и их объединение

Вирусы и ВРЕДОНОСНЫЕ ПРОГРАММЫ

- Дистанционное управление,
- Программы слежения
- Снижение быстродействия
- Баннеры..

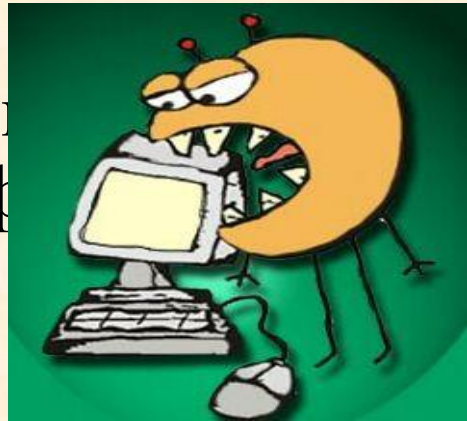
Вред, приносимый вирусами:

- Уничтожение данных,
- Потеря ресурсов ПК,
- Модификация файлов (и писем),
- Бессистемная рассылка файлов и писем,
- Потеря репутации.



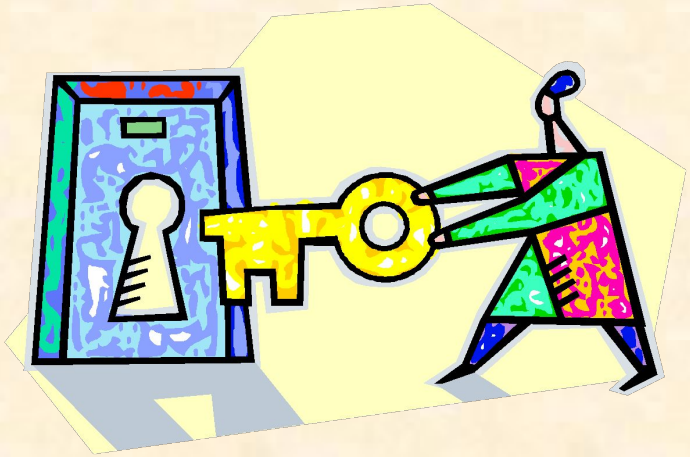
Признаки заражения компьютера

- Прекращение работы или неправильная работа ранее успешно функционировавших программ.
- Медленная работа компьютера.
- Невозможность загрузки операционной системы.
- Исчезновение файлов и каталогов или искажение их содержимого.
- Изменение даты и времени модификации файлов.
- Любые странности в поведении ком включая иногда довольно красивые в/эф



Пути проникновения вирусов в систему

- ☹ **Носители информации**
- ☹ **«Дыры» в ПО**
- ☹ **Неправильная настройка ПО**
- ☹ **Интернет**



Что делать?

- ☺ **Проверять ВСЕ носители информации**
- ☺ **Устанавливать последние версии и обновления**
- ☺ **Анализировать свои действия при настройке**
- ☺ **Устанавливать антивирус на шлюзе**

Компромисс:

защищенность ↔ удобство работы

Виды антивирусных программ…

- Монитор
- Сканер
- Антивирус на шлюзе
- Контроль CRC или ревизор
- Вакцина или иммунизатор
- Антивирусы специального ПО
- Сочетания

…и как их обманывать

1. Скрыть (зашифровать) содержимое от сканера и монитора (полиморфик)
2. Использовать неконтролируемое расширение: rtf, ex_
3. Модифицировать на время проверки (стелс)
4. Уничтожить антивирус
5. Создать новый вирус
6. Спрятать в архиве с паролем

Антивирусная программа

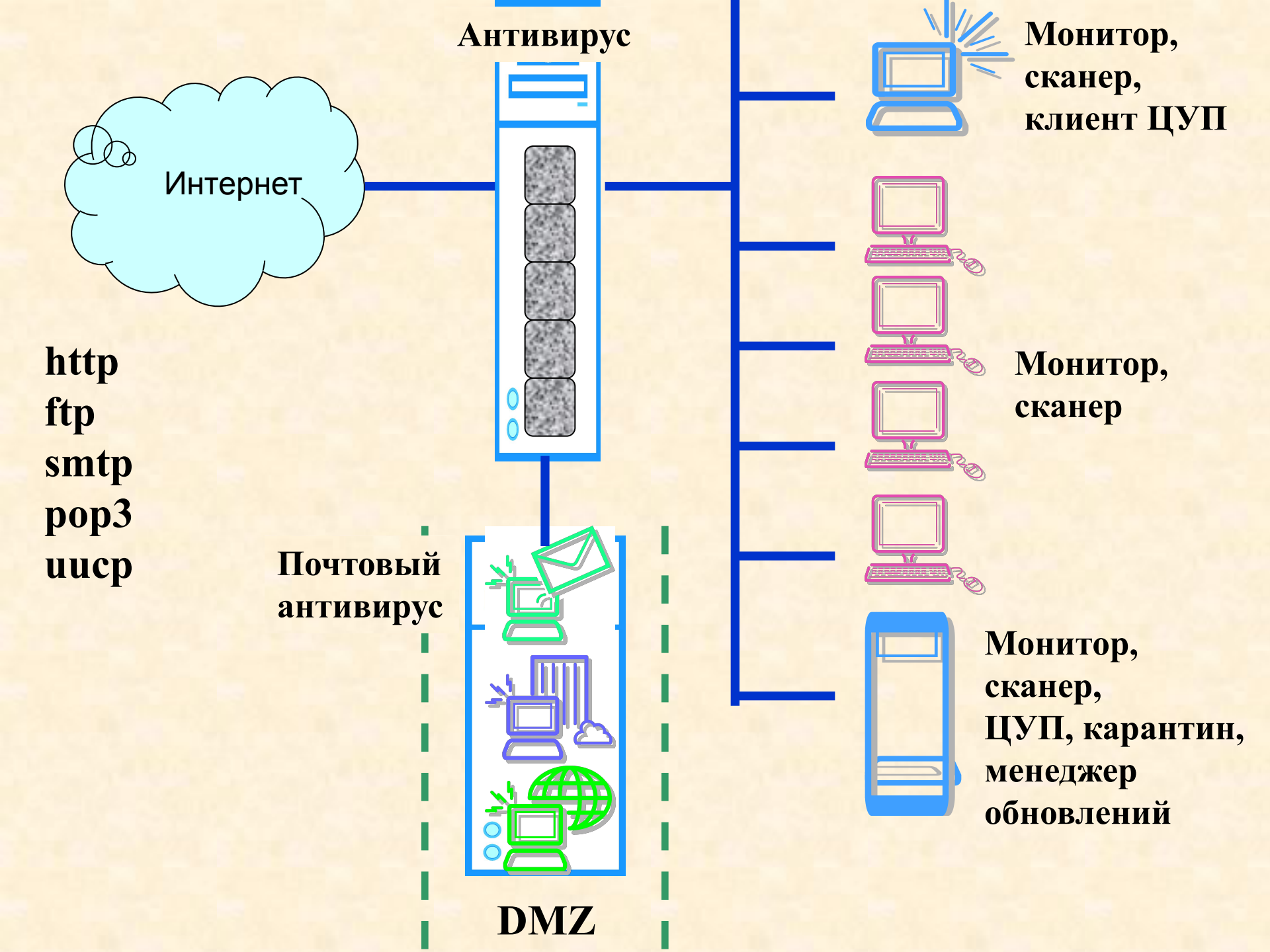
Антивирусная программа	Цены	Обновления	Размер
DrWeb Диалог-наука	б/п для ОУ.	Несколько раз в день, б/п	8 Мб
AVP Лаборатория Касперского	~300 уе на машину	1 раз в день, б/п	14 Мб
Norton Antivirus SYMANTEC Corporation		Раз в несколько дней, б/п	26.8 Мб
Panda Panda		Зарегистрирован-ным пользователям	

Антивирусные ресурсы

- www.DialogNauka.ru
- ftp.dials.ru
- www.avp.ru (www.kaspersky.com)
- www.relans.ru
- www.viruslist.com
- www.pandasoftware.com
- www.symantec.com (http://www.symantec.ru)
- www.trendmicro.com
- www.mcafee.com

Сетевой антивирус

- Централизованное управление всеми настройками.
- Автоматическая установка на рабочих станциях.
- Получение обновлений через сервер сети.
- Удаленный запуск проверки.
- Централизованный просмотр log-файлов.


Антивирус
Интернет
Монитор,
сканер,
клиент ЦУП
http
ftp
smtp
pop3
uucp
Монитор,
сканер
Почтовый
антивирус
Монитор,
сканер,
ЦУП, карантин,
менеджер
обновлений
DMZ

Варианты установки антивирусного обеспечения

ОЗУ > 64 МБ на р.с. + сеть
Сетевая версия любого антивируса с ЦУ

ОЗУ > 64 МБ
DrWeb или AVP с монитором

ОЗУ < 32 МБ
DrWeb, сканер

Установка и настройка

Какие расширения?	Все?
Какие каталоги проверять? Проверять ли сеть?	Все кроме серверных, возможно с базами данных
Проверка на чтение и запись?	Да
Что разрешить настраивать пользователю и как ему это запретить?	Ничего
Сканировать на загрузке?	По минимуму
Сканировать на входе в сеть?	Нет
Проверка CD и floppy?	Да
Проверка наличия floppy	Да кроме notebook

Установка и настройка (2)

Эвристика?	Не рекомендуется
Уровень вложенности архивов	3
Что делать с зараженным письмом?	Удалять/лечить/ Базы не лечить?
Что делать с зараженным файлом?	Лечить, делать копии
Как настроить карантин?	
Как настроить оповещение?	
Расписание обновлений и сканирование	Каждый день
Включать ли обновление soft автоматически	Нет

Инструкция пользователя

Зависит от конфигурации рабочего места!

- Оснастить свой компьютер современной антивирусной программой и постоянно обновлять ее версию
- Проверять новые файлы, если нет монитора
- Периодически проверять жесткие диски компьютера, запуская антивирусы для тестирования файлов, памяти и системных областей дисков
- Не оставлять дискеты в дисководе при перезагрузке
- Сканировать дискеты перед использованием

Инструкция пользователя

- Проверять архивы после разархивации
- Не пытаться обмануть антивирусную программу и все-таки запустить программу, если есть сообщение о вирусе
- Создавать резервные копии важной для вас информации на дискетах
- Иметь boot-дискету
- При наличии локальной сети следовать инструкциям администратора

Думать?

Инструкция администратора

- Проверка файлов-отчетов о работе антивируса
- Желательно отследить источник заразы
- Обеспечить постоянное обновление
- Раздавать AVIR
- Поддерживать в рабочем состоянии 1-2 консольных версий разных антивирусов
- Повышать свою образованность и моральную устойчивость
- Не ругать глупых пользователей
- Принимать меры к “умным” пользователям, пытающихся экспериментировать с вирусами.

Если на компьютере обнаружен вирус (для пользователя)

- Не паниковать
- Запустить антивирусную программу
- Убедиться, что файлы излечены
- Проанализировать, откуда пришел вирус и сообщить о нем
- Обращаться к администратору в сомнительных ситуациях

Если на компьютере обнаружен вирус (для администратора)

- Если антивирус есть, обновить и проверить.
- Сделать технические выводы: почему монитор есть, а заражение произошло, или почему не было проверки сканером на входе.
- Если антивирус не справился:
  - или загрузиться с boot-дискеты или CD и лечить;
  - или посмотреть какие файлы заражены и после загрузки с дискеты уничтожить эти файлы и восстановить их заново (если есть резервные копии).

Приемы авторов вирусов для обмана

1. Двойное расширение файла
2. Очень длинное имя файла
3. Фотография красивой девушки, желающей познакомиться
4. Обновление программного обеспечения (даже антивирусов)
5. Файл, присланный от имени администратора
6. и т.д.

Заблуждения, с которыми надо бороться

- Не ставить сеть – будут вирусы (в сети легче обслуживать антивирусы)
- Зачем бороться с вирусами, если есть системный администратор
- Это не моя машина – мне все равно
- Не подключаться к Internet