Компьютерные вирусы и антивирусные программы

Компьютерный вирус

это

небольшая программа, написанная в машинных кодах, способная внедряться в другие программы, хранящиеся на дисках запоминающих устройств компьютера, и умеющая самовоспроизводиться

Исторические сведения

Первый вирус появился где-то в самом начале 70-х или даже в конце 60-х годов, хотя «вирусом» его никто еще не называл.

В начале 1989г. вирусом, написанным американским студентом Моррисом, были заражены и выведены из строя тысячи компьютеров, в том числе принадлежащих министерству обороны США. Автор вируса был приговорен к трем месяцам тюрьмы и штрафу в 270 тыс. $. Наказание могло быть и более строгим, но суд учел, что вирус не портил данные, а только размножался

Классификация вирусов

по среде обитания

по способу заражения

по особенностям алгоритма

по масштабу воздействия

По среде обитания

Файловые

Загрузочные

Сетевые

Макро-вирусы

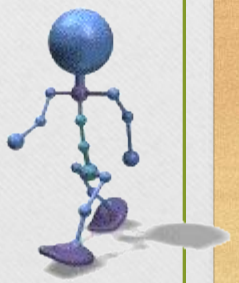
Классификация по среде обитания

Файловые вирусы заражают выполняемые файлы (это наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы заражают загрузочные сектора дисков (boot-сектор), либо главную загрузочную запись (Master Boot Record), либо меняют указатель на активный boot-сектор.

Макро-вирусы - разновидность файловых вирусов встраивающиеся в документы и электронные таблицы популярных редакторов.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.



Среда обитания

По способу заражения

Резидентные

оставляют свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения и внедряются в них. Активные до выключения или перезагрузки компьютера.

Не резидентные

не заражают память компьютера активное неограниченное время

По масштабу воздействия

Безвредные

Неопасные

Очень опасные

Опасные

По масштабу вредных воздействий компьютерные вирусы делятся на:

Безвредные – не влияют на работу ПК, лишь уменьшают объем свободной памяти на диске, в результате своего размножения

Неопасные – влияние, которых ограничивается уменьшением памяти на диске, графическими, звуковыми и другими внешними эффектами;

Опасные – приводят к сбоям и зависаниям при работе на ПК;

Очень опасные – приводят к потери программ и данных (изменение, удаление), форматированию винчестера и тд.

По особенностям алгоритма

Простейшие

Вирусы-черви

Вирусы-невидимки

Квази-вирусы

Стадии вируса

Активная

Пассивная

Активная стадия (атака вируса)

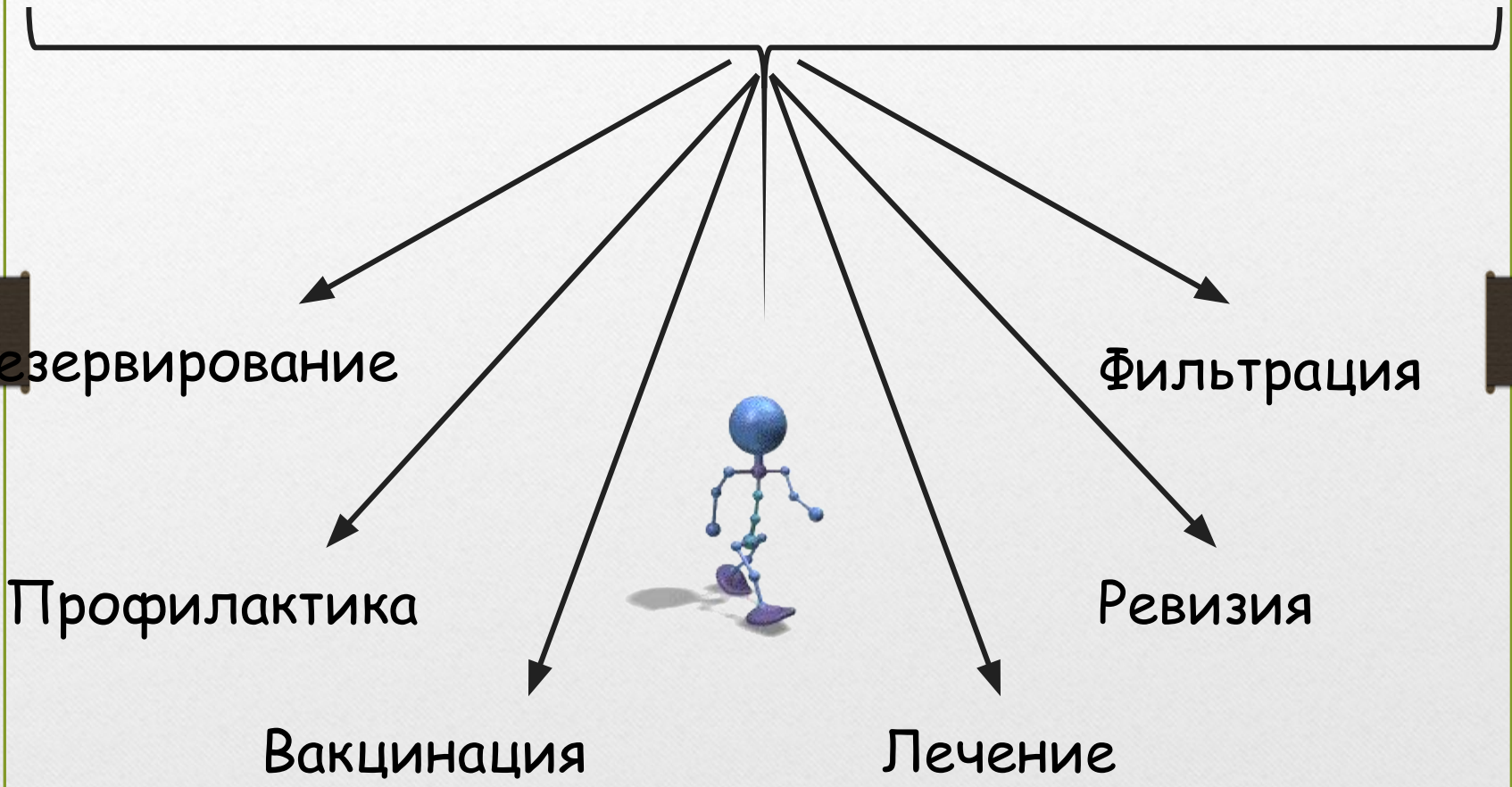
Вирусная атака может начинаться одновременно на всех пораженных компьютерах или в разное время. Обычно атака начинается с выполнения некоторого общего для всех компьютеров условия.

Начало активным действиям вируса может положить достижение определенного количества вызовов зараженной программы на исполнение.

Пассивная стадия

Вирус практически не проявляет себя, стараясь оставаться незаметным для пользователя. Получая управление на этой стадии, вирус отыскивает на других дисках компьютера системные или прикладные программы и внедряется в них. Продолжительность этой фазы может быть разной: от нескольких минут до нескольких лет.

Защита от компьютерных вирусов.



Основными мерами защиты от вирусов считаются:

Резервирование (копирование FAT, ежедневное ведение архивов файлов);

Профилактика (раздельное хранение вновь полученных программ и эксплуатирующихся, хранение неиспользуемых программ в архивах, использование специального диска для записи новых программ);

Ревизия(анализ вновь полученных программ специальными средствами и их запуск в контролируемой среде, систематическая проверка *BOOT*-сектора используемых дискет и содержимого системных файлов (прежде всего *command.com*) и др.);

Фильтрация (использование специальных сервисных программ для разбиения диска на зоны с установленным атрибутом *read only*,);

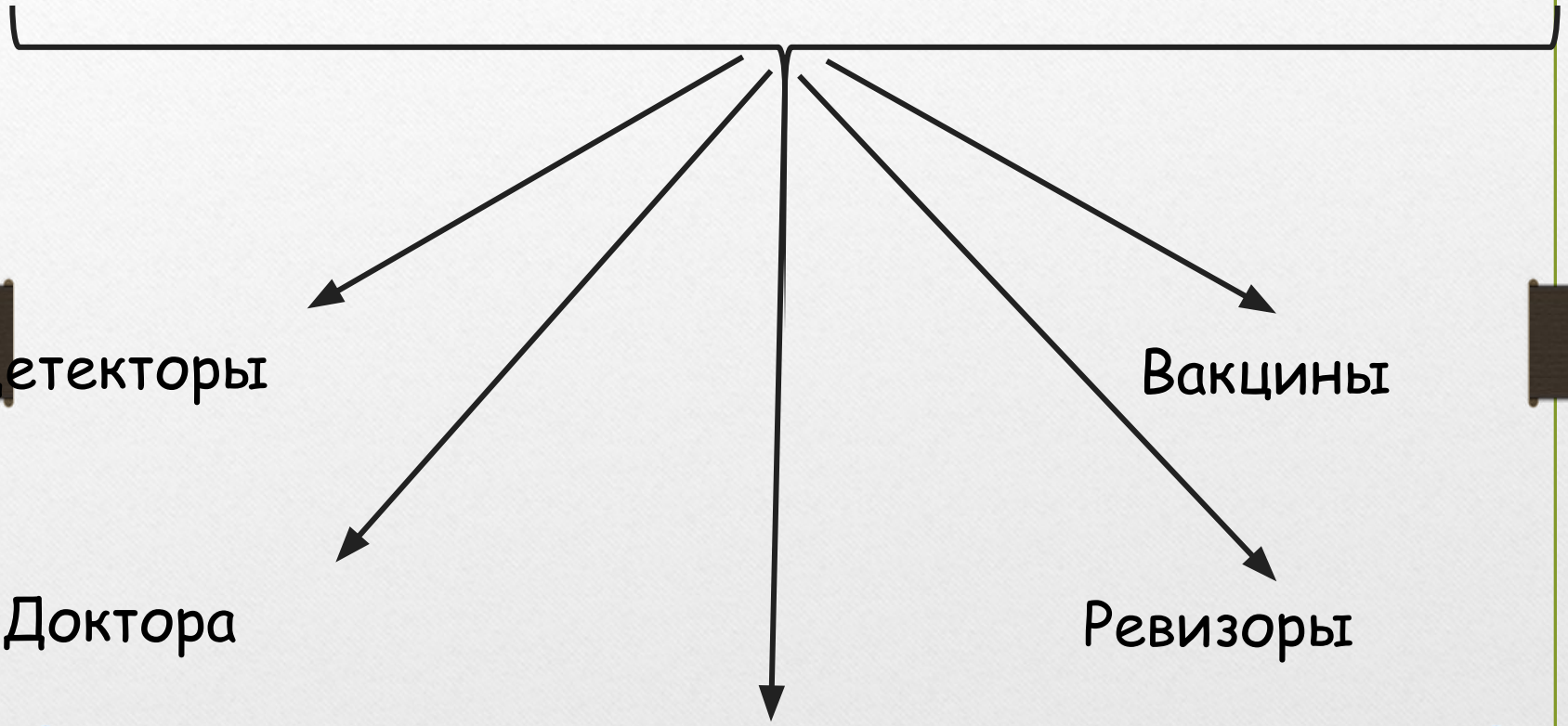
Вакцинация (специальная обработка файлов, дисков, каталогов, запуск специальных резидентных программ-вакцин, имитирующих сочетание условий, которые используются данным типом вируса для определения, заражена уже программа, диск, ЭВМ или нет, т.е. обманывающих вирус);

Лечение (дезактивацию конкретного вируса с помощью специальной программы или восстановление первоначального состояния программ путем удаления всех экземпляров вируса в каждом из зараженных файлов или дисков).

Антивирусные программы

предназначены для предотвращения заражения компьютера вирусом и ликвидации последствий заражения.

Основные антивирусные средства



Антивирусные программы

Сторожа или детекторы – предназначены для обнаружения файлов зараженных известными вирусами, или признаков указывающих на возможность заражения.

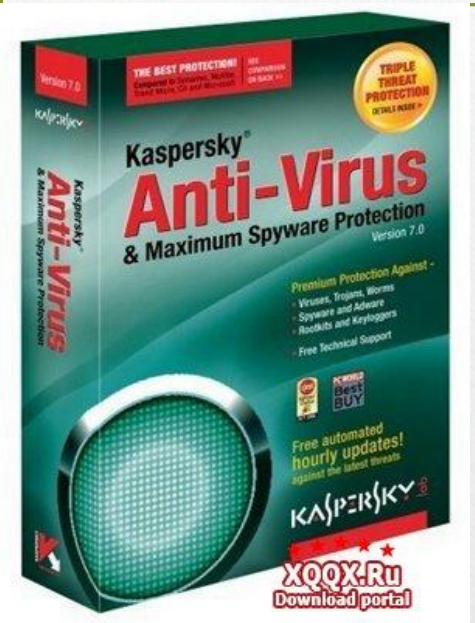
Доктора – предназначены для обнаружения и устранения известных им вирусов, удаляя их из тела программы и возвращая ее в исходное состояние. Наиболее известными представителями являются Dr.Web, AidsTest, Norton Anti Virus.

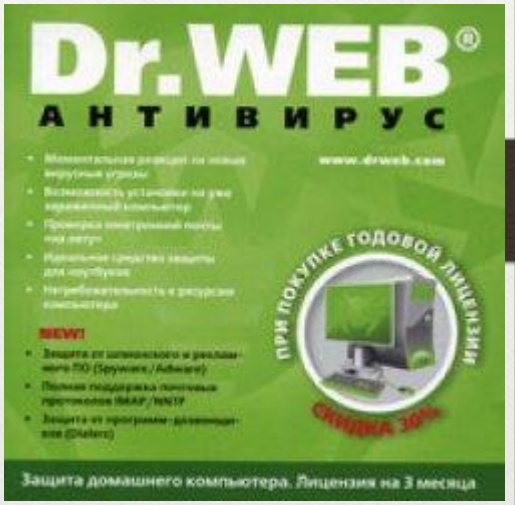
Ревизоры – они контролируют уязвимые и поэтому наиболее атакуемые компоненты компьютера, запоминают состояние служебных областей и файлов, а в случае обнаружения изменений сообщают пользователю.

Резидентные мониторы или фильтры – постоянно находятся в памяти компьютера для обнаружения попыток выполнить несанкционированные действия. В случае обнаружения подозрительного действия выводят запрос пользователю на подтверждение операций.

Вакцины – имитируют заражение файлов вирусами. Вирус будет воспринимать их зараженными и не будет внедряться.

Наиболее известные антивирусные программы

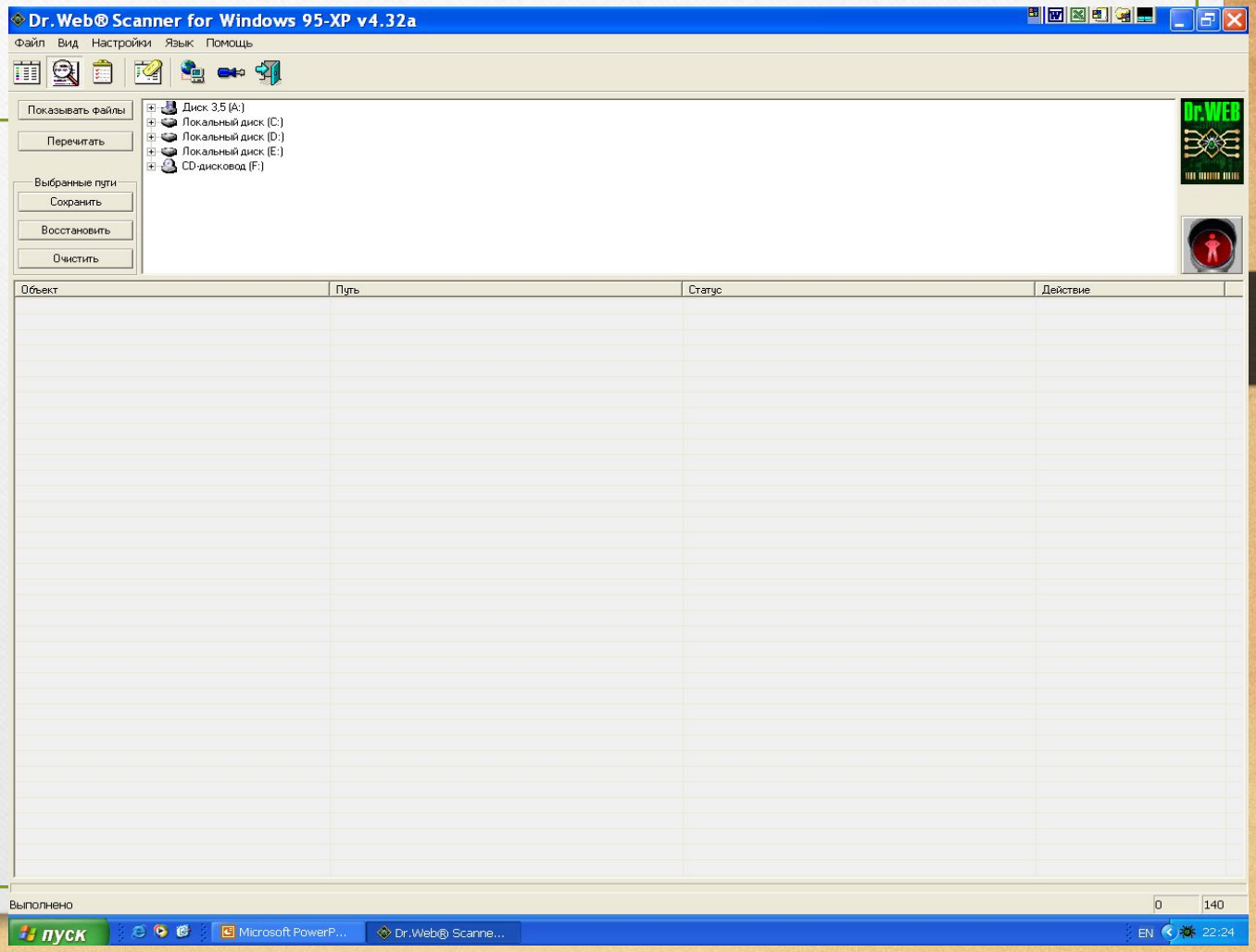




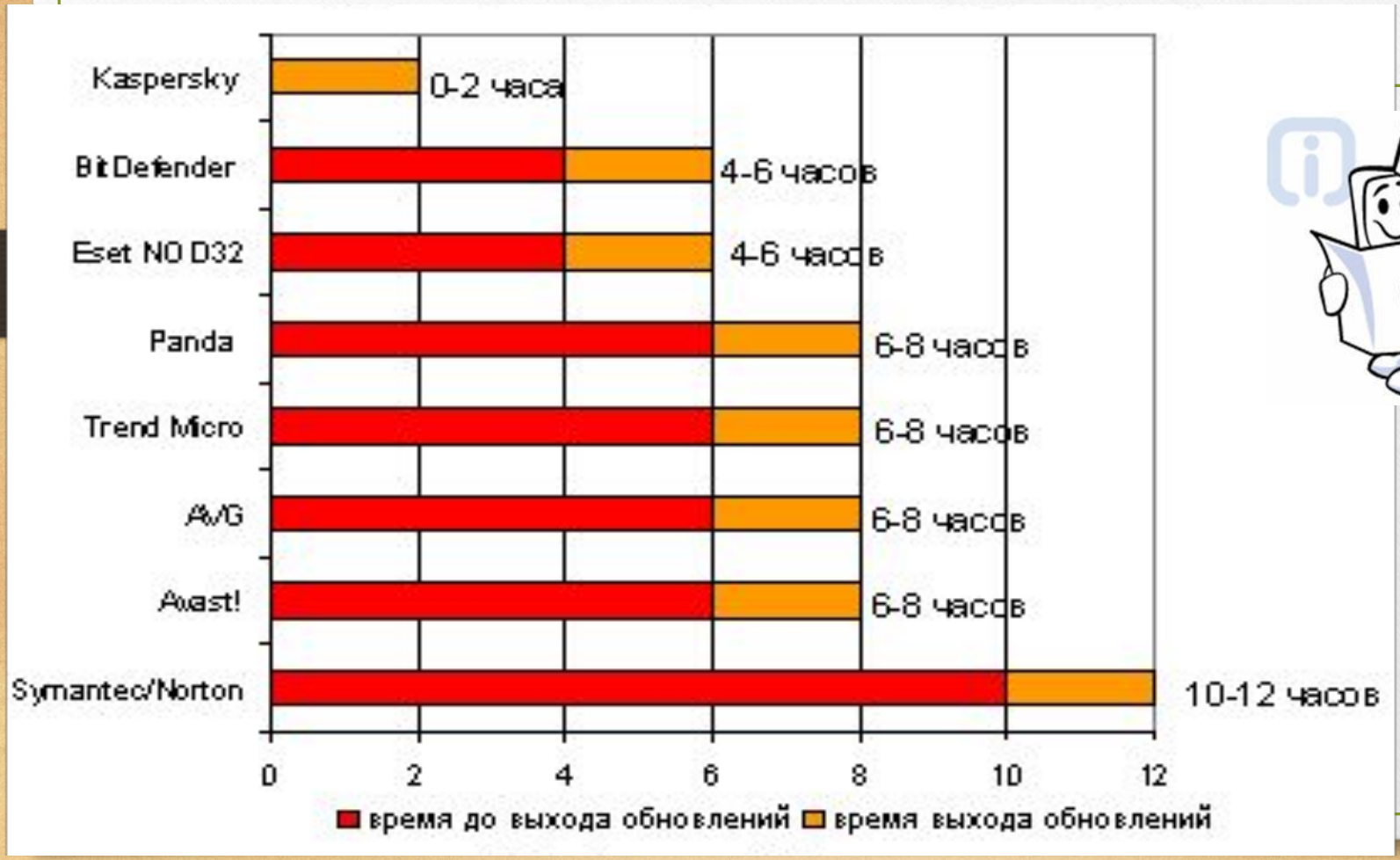
АНТИВИРУС КАСПЕРСКОГО

Антивирусная программа Dr. Web

- Командное меню
- Панель инструментов
- Дерево дисков
- Поле статистики



Среднее время реакции различных антивирусных программ на новые угрозы



Правила компьютерной "гигиены"

- Не использовать сомнительные дискеты
- Ограничить доступ к файлам программ, устанавливая для них, когда возможно, статус «только для чтения»
- При работе в сети, по возможности, не вызывайте программы из памяти других компьютеров.
- Храните программы и данные на разных дискетах или в разных подкаталогах жесткого диска.
- Не копируйте программы для собственных нужд со случайных копий.
- Обязательно иметь антивирусную программу

Обзор урока

На сегодняшний день зарегистрировано более **100000** вредоносных программ или компьютерных вирусов. Если раньше преобладали файловые вирусы и Boot-вирусы, то теперь основная масса вредоносных программ приходится на «почтовые черви» и шпионские программы («троянские кони») с функциями удалённого управления поражённым компьютером.

Антивирусная программа обычно состоит из антивирусного монитора и антивирусного сканера, которые используют общую антивирусную базу данных. Её необходимо регулярно обновлять через Интернет для надёжной защиты своего компьютера.

Домашнее задание:

Подготовиться к **контрольной работе** по темам:

1. Устройство компьютера
2. Данные и программы
3. Файлы и файловая система
4. Графический интерфейс операционных систем и приложений
5. Компьютерные вирусы и антивирусные программы