Вирусы и антивирусные программы

Вирус – от лат. virus - яд

Компьютерный вирус - специально написанная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, прочих файлов и каталогов, создания всевозможных помех в работе компьютера.

Первые случаи массового заражения ПЭВМ вирусами были отмечены в 1986-1987гг

Сначала появился, так называемый Пакистанский вирус -«Brain»

«Brain» **заразил только в США более 18 тыс. компьютеров и, проделав кругосветное путешествие, попал в СССР**

Следующим широко известным вирусом стал вирус Lehigh (Лехайский вирус), распространившийся в одноименном университете США По состоянию на февраль 1989г. только в США этим вирусом было поражено около 4 тыс. ПЭВМ

Классификация компьютерных вирусов

По среде обитания

- ***Файловые***
- ***Загрузочные вирусы***
- **Сетевые**
- ***Макро-вирусы***

По способу заражения

- ***резидентные***
- ***нерезидентные***

Особенности алгоритма работы

- ***Паразитирующие***
- ***Вирусы-невидимки (стелс-вирусы)***
- ***Мутирующие (полиморфик-) вирусы***
- ***Квазивирусные (троянские)***

Деструктивные возможности

- *Безвредные*
- *Неопасные*
- *Опасные*
- *Очень опасные*


Классификация вирусов
Среда обитания
Способ заражения среды обитания
Степень воздействия
Особенности алгоритма
Сетевые
Файловые
Загрузочные
Файлово-загрузочные
Макро
Резидентные
Нерезидентные
Безвредные
Неопасные
Опасные
Очень опасные
Простейшие
Паразитирующие
Репликаторы (черви)
Стелс (невидимки)
Полиморфные (мутанты)
Квазивирусные (троянские)

Сетевые вирусы

Используют для своего распространения команды и протоколы телекоммуникационных сетей.

Попав из сети, они помимо действий на данном компьютере, отыскивают в операционной системе адреса других сетей и отсылают по ним свои копии

Вирусы-черви - это сетевые вирусы (вирусы-репликаторы), распространяются по компьютерным сетям.

Файловые вирусы

Файловые вирусы (program viruses, **программные**) - простейшие в организации вирусы-паразиты, поражающие только программы (файлы, имеющие расширение **.exe** и **.com**, и библиотеки - **.dll**). Размер программы после заражения увеличивается на величину программы-вируса.

Загрузочные вирусы и макровирусы

Загрузочные вирусы поражают загрузочные разделы жестких дисков

Макро-вирусы заражают файлы, имеющие возможность содержать вставки кода программ на VBA.

Резидентные и нерезидентные вирусы

Резидентные вирусы находятся в памяти и являются активными вплоть до выключения ПК.

Нерезидентные вирусы не заражают память ПК и сохраняют активность ограниченное время.

По алгоритмам функционирования

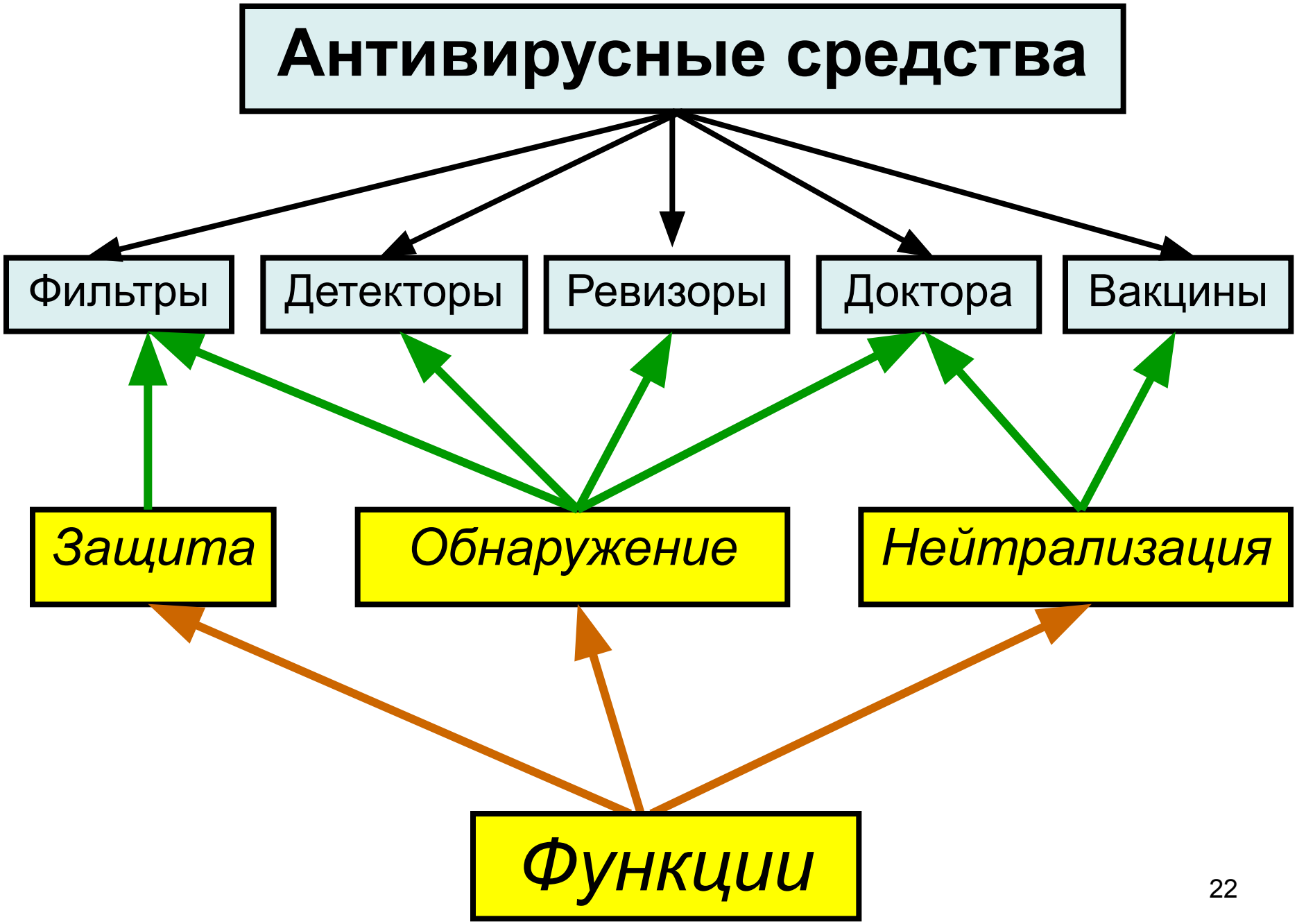
Паразитирующие – вирусы, изменяющие содержимое зараженных файлов. Они легко обнаруживаются и удаляются из файла, имеют всегда один и тот же программный код.

По алгоритмам функционирования

Вирусы-невидимки (***стелс-вирусы***) - это столь хитроумно сделанные вирусы, что их часто невозможно обнаружить с помощью обычных антивирусных средств.

Полиморфик-вирусы (мутирующие вирусы) – это достаточно труднообнаруживаемые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода.

"троянский конь" – программы, которые помимо выполнения основных функций, содержат средства для незаконных операций


Антивирусные средства
Фильтры
Детекторы
Ревизоры
Доктора
Вакцины
Защита
Обнаружение
Нейтрализация
Функции

Антивирусы-***фильтры*** (сторожа) следят за работой ПК и если замечают действия, подозрительно похожие на проявление вируса сообщают об этом пользователю

«Фильтры» реагируют как на известные так и на неизвестные вирусы

Часто выдают запросы на подтверждение какой-либо операции

Не могут обнаружить вирусы, которые запускаются раньше антивируса-фильтра

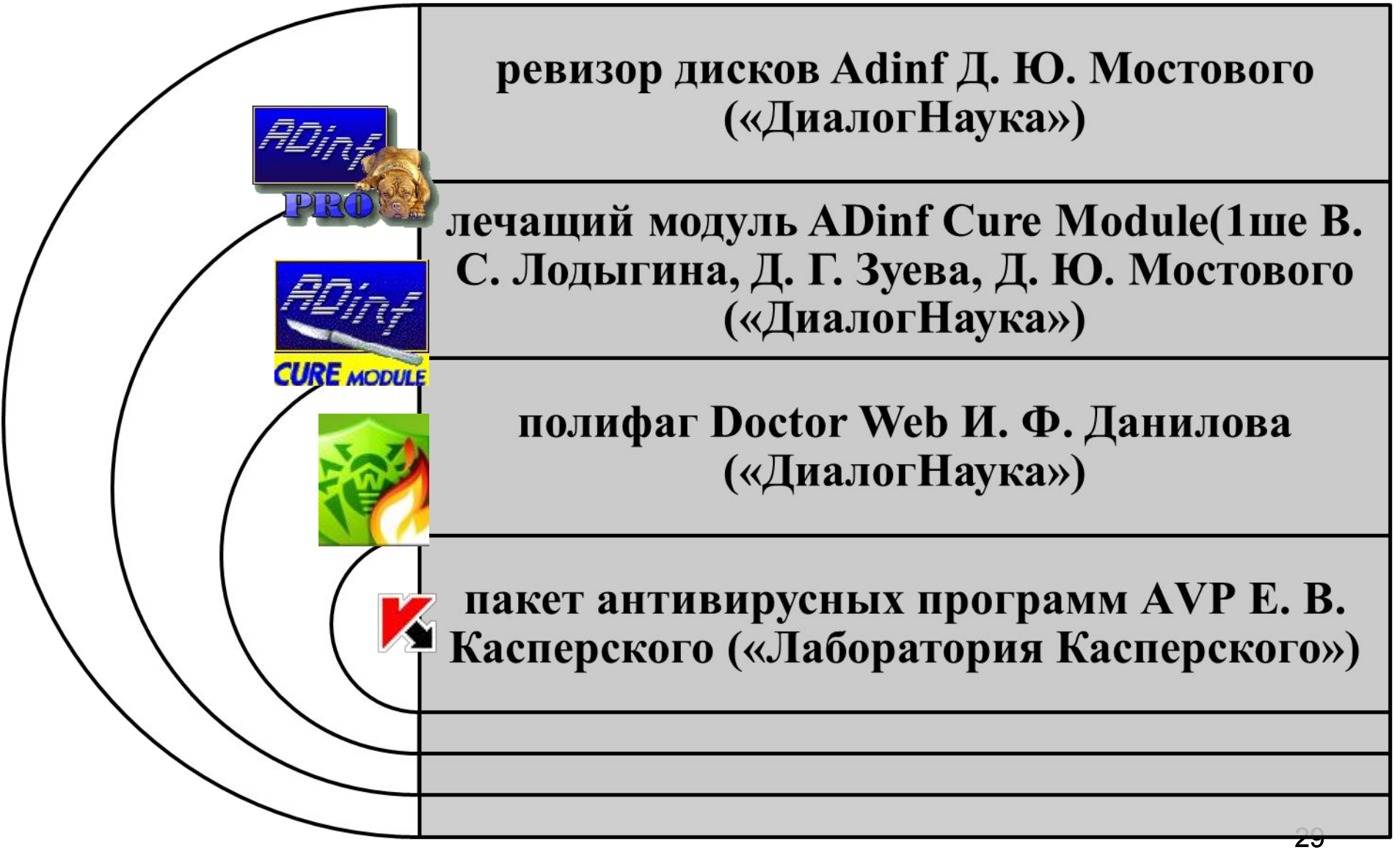
Программы-***детекторы*** осуществляют поиск характерной для конкретного вируса сигнатуры в ОП и в файлах и при обнаружении выдают соответствующее сообщение

Антивирусы-***ревизоры*** запоминают, как "выглядели" программы незараженными и периодически сравнивают эти данные с текущим видом программ. Обнаруженные изменения выводятся на экран монитора.

Программа-*дезинфектор* (**доктор, фаг**) может не только обнаружить, но и попытаться обезвредить вирус

Иммунизатор (**вакцина**) — программа, размещается в памяти резидентно (постоянно) и имитируют наличие в ней вируса, вследствие чего настоящий вирус в памяти не размещается.

Популярные антивирусные программы:



ревизор дисков Adinf Д. Ю. Мостового («ДиалогНаука»)

лечащий модуль ADinf Cure Module(1ше В. С. Лодыгина, Д. Г. Зуева, Д. Ю. Мостового («ДиалогНаука»)

полифаг Doctor Web И. Ф. Данилова («ДиалогНаука»)

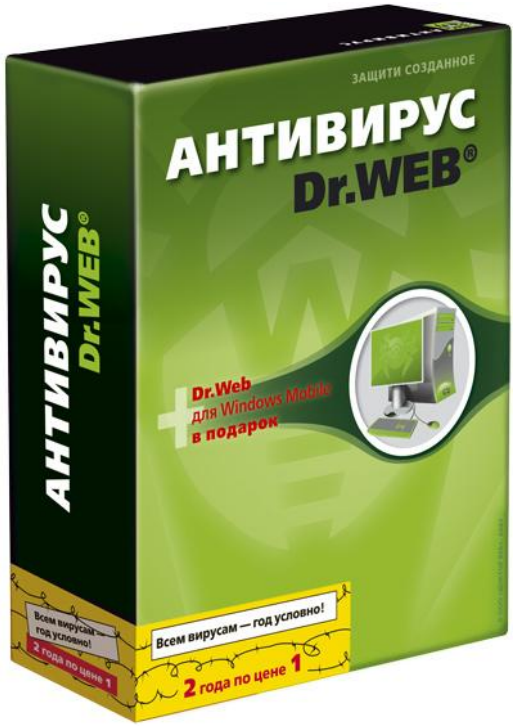
пакет антивирусных программ AVP Е. В. Касперского («Лаборатория Касперского»)

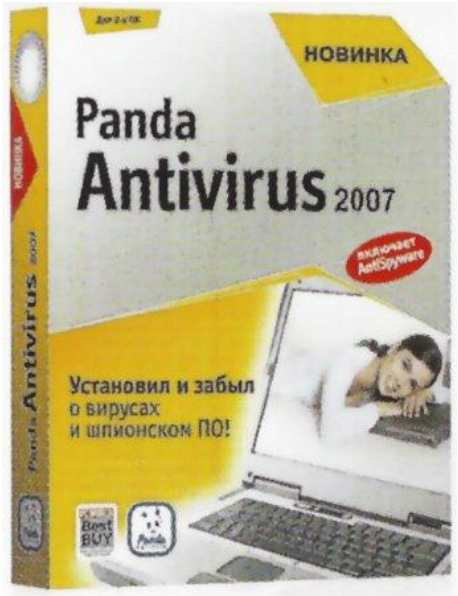
Российские программы

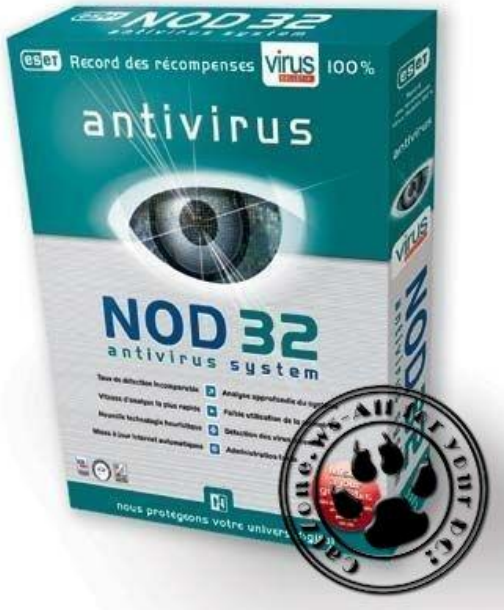
Dr.Web (автор И.Данилов, Диалог-Наука),
ADinf (автор Д.Мостовой, фирма Диалог-Наука, Москва)
AVP Касперского

Aidstest (автор Д.Лозинский, фирма Диалог-Наука, Москва)

Антивирусные программы







зарубежные

Norton AntiVirus
(компания Symantec),
Panda
Dr.Solomon

Одним из направлений развития информатики является

- Компьютерная графика
- Инженерная графика
- Начертательная геометрия
- Теория графов

Антивирусными пакетами являются…

1. Norton AntiVirus
2. Symantec AntiVirus
3. Антивирус Касперского
4. Microsoft AntiVirus

Виды антивирусных программ

1. программы-прививки;
2. программы-вакцины;
3. программы-доктора;
4. программы-врачи
5. программы-детекторы

Протокол Secure Sockets Layer ...

- не может использовать шифрование с открытым ключом
- не использует шифрование данных
- **обеспечивает безопасную передачу данных**
- устраняет компьютерные вирусы