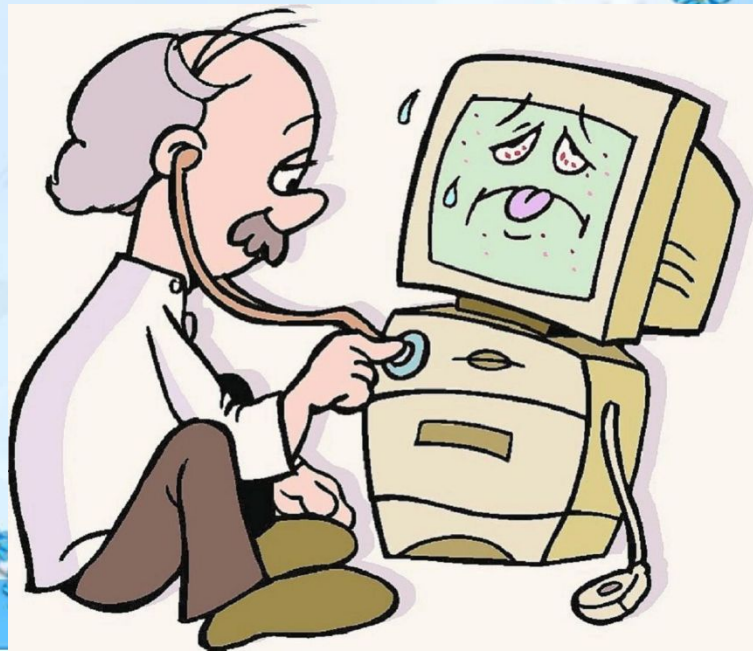
Характеристика антивирусных программ



Различают следующие виды антивирусных программ:

- программы-детекторы;
- программы-доктора или фаги;
- программы-ревизоры;
- программы-фильтры;
- программы-вакцины или иммунизаторы.

ПРОГРАММЫ-ДЕТЕКТОРЫ

Позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов.

Программы-детекторы могут обнаруживать только те вирусы, которые ей "известны". Некоторые программы-детекторы могут настраивать на новые типы вирусов, им необходимо лишь указать комбинации байтов, присущие этим вирусам.

Большинство программ-детекторов имеют функцию "доктора", т.е. они пытаются вернуть зараженные файлы или области диска в их исходное состояние.

Наиболее известные представители этого класса - *AVP (Antiviral Toolkit Pro, автор - Е.Касперский), Aidstest (автор - Д. Лозинский) и Doctor Web (авторы - И. Данилов, В.Лутовинов, Д.Белоусов).*

Программы-доктора

Они не только находят файлы, зараженные вирусами, но и лечат их, удаляя из файла тело программы-вируса. Программы-доктора, которые позволяют лечить большое число вирусов, называются **полифагами**.

ПРОГРАММЫ-РЕВИЗОРЫ

Имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным.

Многие программы-ревизоры являются довольно "интеллектуальными" - они могут отличать изменения в файлах, вызванные, например, переходом к новой версии программы, от изменений, вносимых вирусом, и не поднимают ложной тревоги.

Замечание! Многие программы-ревизоры не умеют обнаруживать заражение "невидимыми" вирусами, если такой вирус активен в памяти компьютера.

Появились очень полезные гибриды ревизоров и докторов, т.е. ДОКТОРА-РЕВИЗОРЫ - программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние.

ПРОГРАММЫ-ФИЛЬТРЫ

Располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.

Преимущество: они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить.

ПРОГРАММЫ-ВАКЦИНЫ, или ИММУНИЗАТОРЫ

Модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.

Выводы по лекции

Программы-детекторы - это программы, которые позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.

Программы-доктора (или полифаги) - это программы, которые находят файлы, зараженные вирусами, лечат их, удаляя из файла тело программы-вируса.

Доктора-ревизоры - это программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние.

Программы-ревизоры - это программы, которые анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора.

Антивирусы-фильтры - это резидентные программы (сторожа), которые оповещают пользователя обо всех попытках какой-либо программы выполнить подозрительные действия.

Вакцинаторы - наименее эффективные антивирусные программы, сильно устаревшие.