**Тема: Антивирусные программы.**

Цели: рассмотреть виды и назначение антивирусных программ, дать им характеристику.

Ход работы:

|  |
| --- |
| *Антивирусная программа* (*антивирус*) – это программа для обнаружения компьютерных вирусов и других вредоносных программ, лечения и восстановления инфицированных файлов, а также для профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом. |

Антивирусные программы обычно используют два различных метода для выполнения своих задач:

1) сканирование (просмотр) файлов для поиска уже известных вирусов, для которых в вирусной базе (входящей в комплект антивирусной программы специальной БД) есть информация о характерных фрагментах вирусного программного кода (сигнатурах вирусов);

2) обнаружение подозрительного поведения любой программы, которое похоже на поведение зараженной программы («эвристическое сканирование»).

Антивирусное программное обеспечение состоит из пакета программ, которые обнаруживают, предотвращают размножение и удаляют компьютерные вирусы и другие вредоносные программы.

При выборе антивирусной программы необходимо учитывать следующие параметры, которым антивирус должен соответствовать:

1. *Постоянство и надежность работы.*  При стабильной работе антивирусной программы нет ощущения, что какие-то зараженные файлы остались незамеченными.

2. *Большой объем и постоянное обновление вирусной базы.* Сюда же относится умение программы быстро опознавать виды вирусов работать с файлами различных типов (архивами, документами), и осуществлять автоматическую проверку всех новых файлов по мере их копирования.

3. *Быстрота работы антивируса и дополнительные функции.* К дополнительным функциям можно отнести наличие эвристического сканирования и возможность лечения зараженных файлов (когда вирусы из них удаляются, а файлы приводятся в исходное состояние, бывшее до их заражения).

4. *Поддержка различных программой многих операционных систем* – многоплатформность. При работе в сетевом варианте немаловажным является также наличие у антивирусной программы серверных модулей, предназначенных для администрирования, и наличие возможности работы на разных серверах.

**Виды антивирусных программ**

В настоящее время не существует единой классификации антивирусных средств защиты компьютеров, однако их можно разделить на пять основных типов.

|  |
| --- |
| *Программы-детекторы* (*сканеры*) обеспечивают поиск и обнаружение конкретных вирусов. Основаны на сравнении специфической последовательности байтов (сигнатур, или масок вирусов), содержащихся в теле вируса, с байтами проверяемых файлов. Их недостатком является то, что они могут находить только вирусы, уже известные разработчикам таких программ. |

*Универсальные детекторы* проверяют неизменность файлов путем подсчета и сравнения их контрольной суммы с эталоном. Эталонная контрольная сумма указывается в документации на программный продукт или подсчитывается в самом начале эксплуатации с помощью специального модуля программы. Недостаток таких детекторов связан с невозможностью определения причин искажения файлов.

*Специализированные детекторы* выполняют поиск известных вирусов по их сигнатуре (повторяющемуся участку кода). Их недостаток состоит в том, что они способны обнаруживать только часть известных вирусов (для которых в их вирусной базе есть сигнатуры) и не могут обнаруживать новые вирусы, еще не занесенные в их вирусную базу.

|  |
| --- |
| Детектор, позволяющий обнаруживать несколько различных видов вирусов, называют *полидетектором*.  *Программы-докторы* (*фаги*, *дезинфекторы*) не только находят файлы, зараженные вирусом, но и лечат их, удаляя из файлов тело вируса и возвращая файлы в исходное состояние. Полифаги – программы-докторы, предназначенные для поиска и уничтожения большого количества разных видов вирусов. |

|  |
| --- |
| *Программы-ревизоры* анализируют текущее состояние файлов и системных областей дисков и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора. При этом проверяется состояние Boot-сектора, FAT, а также длина файлов, код циклического контроля (контрольная сумма файла), дата и время модификации, атрибуты и другие параметры файлов. |

|  |
| --- |
| *Программы-фильтры* – резидентные программы, которые оповещают пользователя обо всех попытках какой-либо программы выполнить подозрительные действия, а пользователь сам принимает решение о разрешении или запрещении выполнения этих действий. Фильтры контролируют обновление программных файлов и системной области дисков, форматирование диска, загрузку программ в ОЗУ. Однако они не способны обезвредить вирус, для этого нужно применять фаги. |

|  |
| --- |
| *Программы-иммунизаторы* (*вакцины*) –  резидентные программы, предотвращающие заражение файлов. Принцип их работы состоит в том, что в программу записываются признаки конкретного вируса, так что подобный вирус считает ее «уже зараженной» и не производит повторное инфицирование. Эти программы наименее эффективны и морально устарели. |

**Практическая работа:**

# Дайте характеристику антивирусным программам:

# Антивирус Касперского

# Dr. Web

# NOD32

# Norton AntiVirus

# Avast

1. Какой антивирус вы используете дома и почему?