БПОУ ВО «Тотемский политехнический колледж»

# Антивирусные программы, назначение и их классификация

# Цели и задачи урока:

**Цель урока:**

- рассмотреть назначение антивирусных программ

**Задачи урока:**

1) рассмотреть понятие «антивирусные программы»
2) привести классификацию антивирусных программ
3) рассмотреть назначение антивирусных программ:
   - 3.1) программы-детекторы
   - 3.2) программы-доктора или фаги
   - 3.3) программы-ревизоры
   - 3.4) программы-фильтры (сторожа)
   - 3.5) программы-вакцины (иммунизаторы)
   - 3.6) программы доктора-ревизоры
4) рассмотреть современные антивирусные программы
5) привести характеристику трем наиболее популярным антивирусным программам: Лаборатория Касперского Лаборатория Касперского Dr.Web Лаборатория Касперского Dr.Web Avast

# Что такое антивирусная программа?

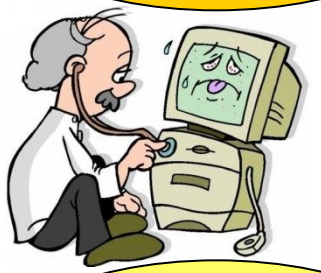
**Антивирусная программа** –

*это компьютерная программа, которая выявляет, предотвращает и выполняет определенные действия, чтобы блокировать или удалять вредоносные программы, такие как вирусы и черви.*

**Количество и разнообразие вирусов велико, и чтобы их быстро и эффективно обнаружить, антивирусная программа должна отвечать некоторым параметрам:**

- ✔ *Стабильность и надежность работы.*
- ✔ *Размеры вирусной базы программы, с регулярным обновлением.*
- ✔ *Возможность программы определять разнообразные типы вирусов, и умение работать с файлами различных типов.*
- ✔ *Наличие резидентного монитора, осуществляющего проверку всех новых файлов автоматически, по мере их записи на диск.*
- ✔ *Скорость работы программы - эвристическое сканирование.*
- ✔ *Возможность восстанавливать зараженные файлы, не стирая их с жесткого диска, а только удалив из них вирусы.*
- ✔ *Процент ложных срабатываний программы.*
- ✔ *Кроссплатформенность.*

# Классификация антивирусных программ



Антивирусные программы

Программы-доктора

Программы-детекторы

Программы-фильтры

Программы-ревизоры

Программы-доктора ревизоры

Программы-вакцины

# Программы-детекторы

***это программы, которые обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях, и при обнаружении выдают соответствующее сообщение.***

Различают детекторы:

- универсальные - используют в своей работе проверку неизменности файлов путем подсчета и сравнения с эталоном контрольной суммы
- специализированные - выполняют поиск известных вирусов по их сигнатуре (повторяющемуся участку кода).

Детектор, позволяющий обнаруживать несколько вирусов, называют ***полидетектором***.

**Недостатком** таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

# Программы-доктора или фаги

***это программы, которые «лечат» зараженные программы или диски, удаляя из зараженных программ тело вируса, т.е. восстанавливая программу в том состоянии, в котором она находилась до заражения вирусом.***

В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к "лечению" файлов.

Среди фагов выделяют **полифаги**, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

**Недостаток:** учитывая, что постоянно появляются новые вирусы, программы-доктора быстро устаревают и требуют регулярного обновления версии.

# Программы-ревизоры

***это программа, запоминающая состояние компьютера, следящая за изменениями файловой системы и сообщающая о важных или подозрительных изменениях пользователю***

Работа программы-ревизора:

- относятся к самым надежным средствам защиты от вирусов.
- запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом.
- затем периодически или по желанию пользователя сравнивают текущее состояние с исходным.
- обнаруженные изменения выводятся на экран монитора.
- сравнение состояний производят сразу после загрузки операционной системы.
- при сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры.

# Программы-фильтры (сторожа)


***представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов.***

Такими действиями могут являться:

- попытки коррекции файлов с расширениями COM и EXE;
- изменение атрибутов файлов;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные сектора диска;
- загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия "сторож" посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения.

**Недостатки:** они не "лечат" файлы и диски, для уничтожения вирусов требуется применить другие программы. Они "назойливы" (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением.

# Программы-вакцины (иммунизаторы)

***это резидентные программы, предотвращающие заражение файлов.***

Программы-вакцины:

- применяют, если отсутствуют программы-доктора, "лечащие" этот вирус.
- вакцинация возможна только от известных вирусов.
- модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится.

**Существенным недостатком** таких программ является их ограниченные возможности по предотвращению заражения от большого числа разнообразных вирусов.

# Программы 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 доктора-ревизоры:

- ✔ могут быть гораздо более универсальными, чем программы-доктора.
- ✔ при лечении они используют заранее сохраненную информацию о состоянии файлов и областей диска. Это позволяет им вылечивать файлы даже от тех вирусов, которые не были созданы на момент написания программы.

**Недостаток.** Они могут лечить не от всех вирусов, а только от тех, которые используют «стандартные», известные на момент написания программы, механизмы заражения файлов.

# Современные антивирусные программы

**Существует большое количество платных и бесплатных АП.**

Среди платных программ можно выделить следующие торговые марки:

- ESET
- Norton Antivirus
- McAfee
- Dr.Web
- Лаборатория Касперского
- NOD32
- BitDefender

Среди условно бесплатных:

- AntiVir (Avira)
- Avast!
- AVG
- Comodo

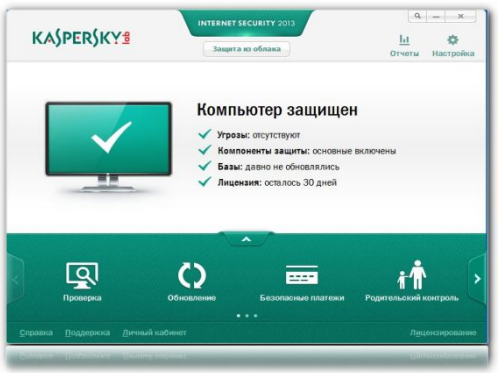

Далее конкретно рассмотрим три известных АП: Лаборатория Касперского Лаборатория Касперского Лаборатория Касперского, Dr.Web Лаборатория Касперского, Dr.Web, Avast

# Антивирусная программа: Лаборатория Касперского

Антиви́рус Каспе́рского (англ. Kaspersky Antivirus, KAV) — антивирусное программное обеспечение, разрабатываемое Лабораторией Касперского, ориентированное на ОС Windows, Linux, Mac OS. Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных угроз с помощью проактивной защиты, включающей компонент HIPS. Первоначально, в начале 1990-х, именовался -V, затем — AntiViral Toolkit Pro. Кроме собственно антивируса, также выпускается бесплатная лечащая утилита Kaspersky Virus Removal Tool.


**Достоинства:**

- ✔ Удобный в пользовании
- ✔ Прекрасно защищает от всех угроз
- ✔ Очень продуманно сделан
- ✔ Достаточно надежный.

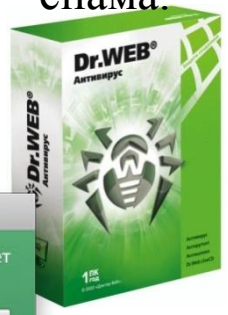



**Недостатки:**

- ✔ Стоит довольно дорого
- ✔ Сильно нагружает систему.

# Антивирусная программа: Dr. Web

**Dr.Web** — семейство антивирусов, предназначенных для защиты от почтовых и сетевых червей, руткитов, файловых вирусов, троянских программ, стелс-вирусов, полиморфных вирусов, бестелесных вирусов, макровирусов, вирусов, поражающих документы MS Office, скрипт-вирусов, шпионского ПО, программ-похитителей паролей, клавиатурных шпионов, программ платного дозвона, рекламного ПО, потенциально опасного ПО, хакерских утилит, программ-люков, программ-шуток, вредоносных скриптов и других вредоносных объектов, а также от спама, скаминг-, фарминг-, фишинг-сообщений и технического спама. Разрабатывается компанией Доктор Веб.





**Достоинства:**

- ✔ Многопоточное сканирование
- ✔ Способность «лечить» от вирусов «зараженные» файлы.

**Недостатки:**

- ✔ Могут быть ложные срабатывания.

# Антивирусная программа: Avast!

Avast! — антивирусная программа для ОС Windows, Linux, Mac OS, а также для КПК на платформе Palm, Android и Windows CE. Разработка компании AVAST Software, основанной в 1991 году в Чехословакии. Для дома выпускается в виде нескольких версий: платной и бесплатной для некоммерческого использования. Также существуют версии для среднего и большого бизнеса и версии для серверов. Продукт сертифицирован ICSA Labs.

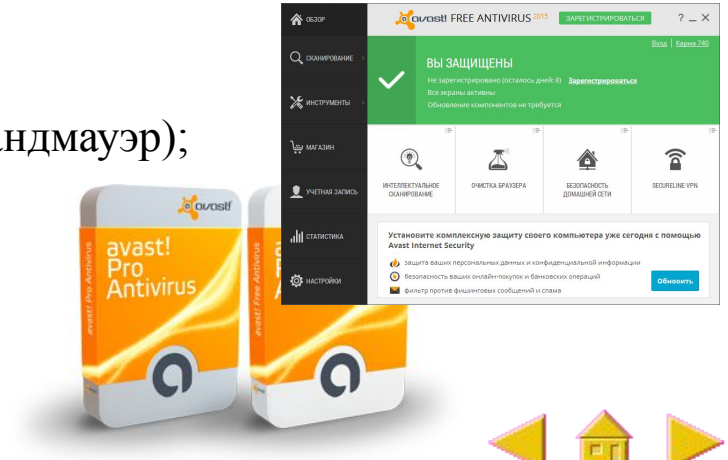
Название avast является сокращением от anti-virus advanced set («продвинутый антивирусный набор»). Avast! Free считается самым популярным бесплатным антивирусом. Всего же антивирусом avast! пользуются более 220 миллионов пользователей во всём мире.

**Достоинства:**

интуитивно понятный, приятный интерфейс;
богатый арсенал (песочница, виртуализация, брандмауэр);
сканирование при загрузке;
низкие требования к ресурсам системы;
доступные цены.

**Недостатки:**

мало обращает внимания на трояны и шпионы.



# Контрольные вопросы:

1) Что такое антивирус? Какие типы антивирусов вы знаете?
2) Какие методы обнаружения компьютерных вирусов вы знаете?
3) Что такое эвристический анализатор? Какие функции он выполняет?
4) Приведите примеры антивирусных программ. Коротко охарактеризуйте их.
5) Какие образом производится лечение зараженных дисков?
6) Что такое программа — детектор?
7) Приведите внешние признаки проявления деятельности вируса.
8) Что такое программа — доктора (фаги)?
9) Что такое программа — ревизоры?
10) Что такое программа — вакцина?
11) Что такое программа — фильтры?
12) Относится ли Dr.Wed к программам-фагам (сканерам)?
13) Какие профилактические действия необходимо совершать для уменьшения вероятности заражения вирусом?
14) Перечислите наиболее распространенные антивирусные программные комплексы.